

# Exhibit A

---



Day Building, Suite 230  
4725 Peachtree Corners Circle,  
Peachtree Corners, GA 30092

Main: (404) 962-8740  
Fax: (404) 962-8741  
[www.ipigrp.com](http://www.ipigrp.com)

February 21, 2020

VIA EMAIL / FEDEX

Ms. Rebecca Baneman  
VP, Litigation  
Altice USA, Inc.  
1111 Stewart Avenue  
Bethpage, NY 11714

**RE: COMMWORKS SOLUTIONS, LLC ("COMMWORKS") - PATENT PORTFOLIO  
LICENSING PROGRAM**

Dear Ms. Baneman:

IPinvestments Group has been retained to manage the monetization of an international patent portfolio owned by CommWorks Solutions, LLC (the "Portfolio"). The Portfolio covers various aspects of telecommunication networks and services, including fiberoptic networks, wireless networks and equipment, mobile networks and devices, telephone networks, voice calling, voicemail, and services provided via the above described networks and equipment. A summary of the Portfolio is detailed below:

- Over 150 active issued patent assets (plus an additional 12 recently expired patent assets)
  - 125+ active issued US assets
  - 20+ active foreign counterparts
- Over 3,500 patent claims
  - Method Claims – 1,500+
  - Apparatus / System Claims – 2,000+
- Over 4,300 forward references

The Portfolio is included in the attached Exhibit A.

While IPinvestments Group is serving as the licensing agent for the CommWorks Portfolio, CommWorks has retained the law firm of Kheyfits Belenky LLP to serve as outside litigation / licensing counsel. Our purpose in writing to Altice USA ("Altice") is to acquaint you with the CommWorks Portfolio and to open a dialogue for Altice to obtain a license under the CommWorks Portfolio prior to any potential enforcement action being initiated. To facilitate licensing discussions, we have attached a mutual NDA for your review and consideration. CommWorks is prepared to grant Altice coverage



Ms. Rebecca Baneman  
February 21, 2020  
Page 2

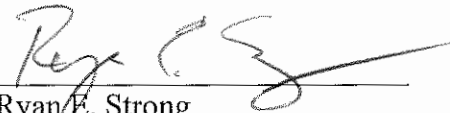
---

under the Portfolio for past and future use to allow you to continue providing and using the technologies. Once the NDA is in place and fully executed, we can provide additional information on potential licensing terms and conditions for the Portfolio.

Over the past few years, we have had the opportunity to represent both small and large companies in their efforts to license their patent portfolios. All too often, it seems, initial licensing efforts are ignored and the burden, time and expense of needless prolonged litigation results. In that spirit, CommWorks believes that early licensing discussions could serve to benefit both parties and would be willing to offer more favorable terms to those that entertain such discussions.

If you would like to participate in discussions regarding a license to the Portfolio or if you have any questions, please contact me at (404) 962-8743 or via email at [rstrong@ipigrp.com](mailto:rstrong@ipigrp.com). The CommWorks licensing team looks forward to hearing from you and working with you to resolve this matter.

Sincerely,

  
Ryan E. Strong

cc: Dmitry Kheyfits, Esq., Kheyfits Belenky, LLP

Enclosures

## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
<u>Active Issued Patents:</u>					
6427001	09/874998	SYSTEM AND METHOD FOR NOTIFICATION OF 911 TELEPHONE CALLS USING LINK MONITORING SYSTEM	US	6/7/2001	7/30/2002
6433742	09/693465	DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS	US	10/19/2000	8/13/2002
6438367	09/710614	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS	US	11/9/2000	8/20/2002
6456242	09/799411	CONFORMAL BOX ANTENNA	US	3/5/2001	9/24/2002
6456245	09/735977	CARD-BASED DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS	US	12/13/2000	9/24/2002
6456764	09/668372	Optical directional coupler	US	9/25/2000	9/24/2002
6483634	09/662904	Optical amplifier	US	9/15/2000	11/19/2002
6487406	09/545619	PCS-to-mobile IP internetworking	US	4/10/2000	11/26/2002
6490067	09/860078	MULTI-CHANNEL OPTICAL TRANSCEIVER	US	5/16/2001	12/3/2002
6490259	09/512514	Active link layer and intra-domain mobility for IP networks	US	2/24/2000	12/3/2002
6505163	09/634794	NETWORK AND METHOD FOR PROVIDING AN AUTOMATIC RECALL TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY	US	8/9/2000	1/7/2003
6594356	10/014918	Initiating a controlling service	US	12/14/2001	7/15/2003
6621854	08/003996	SPREAD-SPECTRUM ELECTROMAGNETIC SIGNALS	US	1/15/1993	9/16/2003
6628943	09/512645	Mobility management utilizing active address propagation	US	2/24/2000	9/30/2003
6636742	09/599201	TRACKING OF MOBILE TERMINAL EQUIPMENT IN A MOBILE COMMUNICATIONS SYSTEM	US	6/22/2000	10/21/2003
6665495	09/698666	NON-BLOCKING, SCALABLE OPTICAL ROUTER ARCHITECTURE AND METHOD FOR ROUTING OPTICAL TRAFFIC	US	10/27/2000	12/16/2003
6724883	09/660133	Processing of data message in a network element of a communications network	US	9/12/2000	4/20/2004
6748064	09/749994	SYSTEMS AND METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS	US	12/28/2000	6/8/2004
6754323	10/025722	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG	US	12/19/2001	6/22/2004
6771971	09/764696	SUBSCRIBER INFORMATION SERVICE CENTER (SISC)	US	1/18/2001	8/3/2004
6775253	09/512644	Adaptive signaling for wireless packet telephony	US	2/24/2000	8/10/2004
6775258	09/527786	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system	US	3/17/2000	8/10/2004
6785534	09/832011	PREPAID/POSTPAID AUTOMATIC CHANGE OF PAYMENT OPTION	US	4/11/2001	8/31/2004



## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
6788660	09/512646	Adaptive mobile signaling for wireless internet telephony	US	2/24/2000	9/7/2004
6792094	09/863477	INTELLIGENT CALL CONNECTION SERVICE	US	5/23/2001	9/14/2004
6795530	09/606062	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS	US	6/29/2000	9/21/2004
6804713	09/549687	Operational supervisory system for a server	US	4/14/2000	10/12/2004
6832249	09/860801	GLOBALY ACCESSIBLE COMPUTER NETWORK-BASED BROADBAND COMMUNICATION SYSTEM WITH USER-CONTROLLABLE QUALITY OF INFORMATION DELIVERY AND FLOW PRIORITY	US	5/18/2001	12/14/2004
6836466	09/579371	Method and system for measuring IP performance metrics	US	5/26/2000	12/28/2004
6857007	09/723349	Personal digital assistant facilitated communication system	US	11/27/2000	2/15/2005
6859529	10/082386	Method and system for self-service scheduling of inbound inquiries	US	2/25/2002	2/22/2005
6865237	09/676373	Method and system for digital signal transmission	US	9/29/2000	3/8/2005
6866587	09/669479	WIDE AREA REAL-TIME SOFTWARE ENVIRONMENT	US	9/25/2000	3/15/2005
6868268	09/896835	AUDIO CALLING NAME AND NUMBER DELIVERY	US	6/29/2001	3/15/2005
6891807	10/341847	Time based wireless access provisioning	US	1/13/2003	5/10/2005
6901437	09/684047	Mobile cache for dynamically composing user-specific information	US	10/6/2000	5/31/2005
6917605	09/770019	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION CHANGING METHOD	US	1/25/2001	7/12/2005
6931003	09/753743	PACKET PRIORITIZATION PROTOCOL FOR A LARGE-SCALE, HIGH SPEED COMPUTER NETWORK	US	12/27/2000	8/16/2005
6956941	09/547627	METHOD AND SYSTEM FOR SCHEDULING INBOUND INQUIRIES	US	4/12/2000	10/18/2005
6967951	10/044244	SYSTEM FOR REORDERING SEQUENCED BASED PACKETS IN A SWITCHING NETWORK	US	1/11/2002	11/22/2005
6975855	09/958065	Method for managing mobile station facilities	US	4/26/2000	12/13/2005
6980089	09/924730	Non-intrusive coupling to shielded power cable	US	8/8/2001	12/27/2005
6985724	10/239763	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes	US	2/27/2001	1/10/2006
7006579	10/023924	ISI-robust slot formats for non-orthogonal-based space-time block codes	US	12/18/2001	2/28/2006
7027465	10/167986	A Method for contention free traffic detection	US	6/11/2002	4/11/2006
7051116	09/983042	Client device identification when communicating through a network address translator device	US	10/22/2001	5/23/2006
7061379	10/301846	RFID system and method for ensuring safety of hazardous or dangerous substances	US	11/21/2002	6/13/2006
7062475	10/715218	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT	US	11/17/2003	6/13/2006
7069483	10/437128	System and method for identifying nodes in a wireless mesh network	US	5/13/2003	6/27/2006

## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
7079823	09/980027	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION	US	5/26/2000	7/18/2006
7092986	10/067278	Transparent Mobile IPV6 Agent	US	2/7/2002	8/15/2006
7106697	10/114925	METHOD FOR DYNAMICALLY COMPUTING A SWITCHING SCHEDULE	US	4/3/2002	9/12/2006
7124435	10/040933	Information management system and method	US	10/23/2001	10/17/2006
7145867	10/114564	SYSTEM AND METHOD FOR SLOT DEFLECTION ROUTING	US	4/2/2002	12/5/2006
7177285	10/961959	Time based wireless access provisioning	US	10/8/2004	2/13/2007
7184444	10/138760	SYSTEM AND METHOD FOR PACKET CLASSIFICATION	US	5/3/2002	2/27/2007
7190900	10/063301	NON-BLOCKING ALL-OPTICAL SWITCHING NETWORK DYNAMIC DATA SCHEDULING SYSTEM AND IMPLEMENTATION METHOD	US	4/9/2002	3/13/2007
7206806	09/870536	Method and system for remote utilizing a mobile device to share data objects	US	5/30/2001	4/17/2007
7209950	09/921167	Method and apparatus for a network independent short message delivery system	US	8/2/2001	4/24/2007
7218637	10/114928	System For Switching Data Using Dynamic Scheduling	US	4/3/2002	5/15/2007
7224642	11/340733	Wireless sensor data processing systems	US	1/26/2006	5/29/2007
7245201	10/947929	Power line coupling device and method of using the same	US	9/23/2004	7/17/2007
7248148	11/265230	Power line coupling device and method of using the same	US	11/3/2005	7/24/2007
7254709	10/699632	Managed information transmission of electronic items in a network environment	US	11/1/2003	8/7/2007
7355961	11/070624	Method and arrangement for digital signal transmission using layered space-time codes	US	3/2/2005	4/8/2008
7363030	10/852528	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG	US	5/24/2004	4/22/2008
7412514	09/932431	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK	US	8/17/2001	8/12/2008
7443790	11/368867	System and method for slot deflection routing at optical router/switch	US	3/6/2006	10/28/2008
7451365	11/425114	System and Method for Identifying Nodes in a Wireless Network	US	6/19/2006	11/11/2008
7460609	10/739017	Transmission method using complex channel symbols	US	12/19/2003	12/2/2008
7463596	11/673513	TIME BASED WIRELESS ACCESS PROVISIONING	US	2/9/2007	12/9/2008
7474853	11/299889	NON-BLOCKING ALL-OPTICAL SWITCHING NETWORK DYNAMIC DATA SCHEDULING SYSTEM AND IMPLEMENTATION METHOD	US	12/12/2005	1/6/2009
7484005	11/351116	Client device identification when communicating through a network address translator device	US	2/10/2006	1/27/2009
7496033	11/453755	Method for dynamically computing a switching schedule	US	6/15/2006	2/24/2009
7526203	10/659485	Apparatus and method for optical switching at an optical switch fabric	US	9/10/2003	4/28/2009
7555273	11/330275	BANDPASS FILTER WITH CARRIER FREQUENCY REDUCTION	US	1/11/2006	6/30/2009
7564863	11/504144	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION	US	8/14/2006	7/21/2009



## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
7596533	11/467888	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT	US	8/28/2006	9/29/2009
7609712	11/504967	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION	US	8/15/2006	10/22/2009
7715712	12/185198	SYSTEM AND METHOD FOR IMPLEMENTING DYNAMIC SCHEDULING OF DATA IN A NON-BLOCKING ALL-OPTICAL SWITCHING NETWORK	US	8/4/2008	5/11/2010
7734807	12/189417	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK	US	8/11/2008	6/8/2010
7760664	11/101136	Determining and provisioning paths in a network	US	4/7/2005	7/20/2010
7814230	12/337854	Client device identification when communicating through a network address translator device	US	12/18/2008	10/12/2010
7835350	11/180764	PRIORITIZING DATA TRANSMISSIONS USING THE NUMBER OF ASSOCIATED ORIGIN ADDRESSES	US	7/13/2005	11/16/2010
7835372	11/421998	System and Method for Transparent Wireless Bridging of Communication Channel Segments	US	6/2/2006	11/16/2010
7835897	11/557064	APPARATUS AND METHOD FOR CONNECTING HARDWARE TO A CIRCUIT SIMULATION	US	11/6/2006	11/16/2010
7852796	11/420668	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION	US	5/26/2006	12/14/2010
7856011	11/237482	Reordering packets	US	9/27/2005	12/21/2010
7869427	11/796682	System For Switching Data Using Dynamic Scheduling	US	4/27/2007	1/11/2011
7911979	12/323399	TIME BASED ACCESS PROVISIONING SYSTEM AND PROCESS	US	11/25/2008	3/22/2011
7937081	12/720862	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	3/10/2010	5/3/2011
7941149	11/615582	Multi-Hop Ultra Wide Band Wireless Network Communication	US	12/22/2006	5/10/2011
7957356	11/462663	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS	US	8/4/2006	6/7/2011
8031800	10/450997	Transmitting digital signal	US	12/19/2001	10/4/2011
8107377	12/759221	Reordering packets	US	4/13/2010	1/31/2012
8116315	11/471149	SYSTEM AND METHOD FOR PACKET CLASSIFICATION	US	6/20/2006	2/14/2012
8117068	12/464782	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK	US	5/12/2009	2/14/2012
8160863	10/044217	System and method for connecting a logic circuit simulation to a network	US	11/19/2001	4/17/2012
8175613	11/741630	SYSTEMS AND METHODS FOR DETERMINING LOCATION OF DEVICES WITHIN A WIRELESS NETWORK	US	4/27/2007	5/8/2012
8195442	12/946721	Use of hardware peripheral devices with software simulations	US	11/15/2010	6/5/2012
8200211	13/097709	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	4/29/2011	6/12/2012
8224909	12/369785	Personal digital assistant facilitated communication system	US	2/12/2009	7/17/2012
8351924	13/484583	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	5/31/2012	1/8/2013
8380481	13/487750	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION	US	6/4/2012	2/19/2013

## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
8423630	10/978953	Responding to quality of service events in a multi-layered communication system	US	11/1/2004	4/16/2013
8533278	13/490403	Mobile computing device based communication systems and methods	US	6/6/2012	9/10/2013
8600372	13/682230	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	11/20/2012	12/3/2013
8611320	12/950558	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS	US	11/19/2010	12/17/2013
8671216	12/795597	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK	US	6/7/2010	3/11/2014
8719326	11/188095	Adaptive data transformation engine	US	7/22/2005	5/6/2014
8780770	11/741637	SYSTEMS AND METHODS FOR VOICE AND VIDEO COMMUNICATION OVER A WIRELESS NETWORK	US	4/27/2007	7/15/2014
8812665	13/781130	GLOBALY ACCESSIBLE COMPUTER NETWORK-BASED BROADBAND COMMUNICATION SYSTEM WITH USER-CONTROLLABLE QUALITY OF INFORMATION DELIVERY AND FLOW PRIORITY	US	2/28/2013	8/19/2014
8913618	13/337717	Reordering packets	US	12/27/2011	12/16/2014
8923846	14/058473	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	10/21/2013	12/30/2014
9230039	14/223936	Adaptive data transformation engine	US	3/24/2014	1/5/2016
9432842	14/549714	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	11/21/2014	8/30/2016
9554304	14/090760	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS	US	11/26/2013	1/24/2017
9648122	11/133755	Mobile cache for dynamically composing user-specific information	US	5/19/2005	5/9/2017
9918222	15/226422	RECOVERY TECHNIQUES IN MOBILE NETWORKS	US	8/2/2016	3/13/2018
9930575	15/409896	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS	US	1/19/2017	3/27/2018
10051077	15/486546	Mobile cache for dynamically composing user-specific information	US	4/13/2017	8/14/2018
RE42122	11/971456	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS	US	1/9/2008	2/8/2011
RE42227	12/481943	Apparatus and method for connecting hardware to a circuit simulation	US	6/10/2009	3/15/2011
RE42232	11/376700	RF CHIPSET ARCHITECTURE	US	3/15/2006	3/22/2011
RE42539	11/727638	NETWORK AND METHOD FOR PROVIDING A CALLING NAME	US	3/27/2007	7/12/2011
RE42883	12/001975	TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY	US	12/13/2007	11/1/2011
RE43704	12/608732	Enhanced Phone-Based Collaboration	US	10/29/2009	10/2/2012
		Determining and provisioning paths within a network of communication elements	US		

## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
RE43746	13/166702	Method and radio system for digital signal transmission using complex space-time codes	US	6/22/2011	10/16/2012
RE44904	13/171882	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION	US	6/29/2011	5/20/2014
CA2310783	CA2310783	PCS-to-mobile IP internetworking	CA	6/6/2000	2/3/2004
CA2581734	CA2581734	Determining and provisioning paths in a network	CA	9/28/2005	8/28/2012
CN2100808958.2	CN00808958.2	INITIATING A CONTROLLING SERVICE	CN	6/13/2000	11/10/2004
DE60037651.6	DE60037651.6	OPTICAL ADD/DROP MULTIPLEXER	DE	2/4/2000	1/2/2008
DE60042650.5	DE60042650.5	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE	DE	6/13/2000	7/29/2009
DE60121094.8	DE60121094.8	Mobile network system and service control information changing method	DE	1/31/2001	6/28/2006
DE60123282.8	DE60123282.8	Transmitting digital signal	DE	12/19/2001	10/11/2007
DE602005053126.2	DE602005053126.2	Determining and provisioning paths in a network	DE	9/28/2005	11/22/2017
DE60244331.8	DE60244331.8	Transmission method	DE	6/24/2002	1/2/2013
ES1192811	ES00942154.6	INITIATING A CONTROLLING SERVICE	ES	6/13/2000	7/29/2009
FR1150530	FR01102111.0	Mobile network system and service control information changing method	FR	1/31/2001	6/28/2006
FR1151567	FR00903718.5	OPTICAL ADD/DROP MULTIPLEXER	FR	2/4/2000	1/2/2008
FR1405453	FR02743313.5	Transmission method	FR	6/24/2002	1/2/2013
GB1150530	GB01102111.0	Mobile network system and service control information changing method	GB	1/31/2001	6/28/2006
GB1151567	GB00903718.5	OPTICAL ADD/DROP MULTIPLEXER	GB	2/4/2000	1/2/2008
GB1192811	GB00942154.6	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE	GB	6/13/2000	7/29/2009
GB1350354	GB01273305.1	Transmitting digital signal	GB	12/19/2001	9/20/2006
GB1405453	GB02743313.5	Transmission method	GB	6/24/2002	1/2/2013
GB1797670	GB05857725.5	Determining and provisioning paths in a network	GB	9/28/2005	11/22/2017
IT1192811	IT502009901774577	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE	IT	6/13/2000	7/29/2009
JP4294829	JP2000-125968	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION REVISION METHOD	JP	4/26/2000	4/17/2009
JP4777990	JP2007-534687	Determining and provisioning paths in a network	JP	9/28/2005	7/8/2011
JP4874550	JP2004-572210	System and method for routing packets in a wired or wireless network	JP	10/31/2003	12/2/2011
TW1183532	TW089110383	PCS-to-mobile IP internetworking	TW	5/29/2000	8/11/2003



## CommWorks Solutions - Exhibit A

Patent Number	Application Number	Title	Country	Application Date	Grant Date
<u>Recently Expired Patents:</u>					
6335821	09/501606	Optical fiber amplifier and a method for controlling the same	US	2/10/2000	1/1/2002
6341221	09/702495	Method of managing a subscriber service by an intelligent network service	US	10/31/2000	1/22/2002
6427037	09/497235	Two-stage optical switch circuit network	US	2/3/2000	7/30/2002
6678080	09/923845	OPTICAL ADD/DROP MULTIPLEXER	US	8/7/2001	1/13/2004
6711122	09/500750	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION	US	2/8/2000	3/23/2004
6721415	09/506021	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER	US	2/17/2000	4/13/2004
6721787	09/501204	SYSTEM AND METHOD FOR WIRELESS HOT-SYNCHRONIZATION OF A PERSONAL DIGITAL ASSISTANT	US	2/10/2000	4/13/2004
6754716	09/502155	RESTRICTING COMMUNICATION BETWEEN NETWORK DEVICES ON A COMMON NETWORK	US	2/11/2000	6/22/2004
7023978	10/818817	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER	US	4/6/2004	4/4/2006
7180850	10/762197	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION	US	1/20/2004	2/20/2007
7626918	11/504252	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION	US	8/14/2006	12/1/2009
RE43163	11/318396	HIGH-SPEED NETWORK OF INDEPENDENTLY LINKED NODES	US	12/22/2005	2/7/2012



## MUTUAL NONDISCLOSURE AGREEMENT

This MUTUAL NONDISCLOSURE AGREEMENT is made and entered into as of \_\_\_\_\_, 20\_\_\_\_  
between CommWorks Solutions, LLC, a Georgia company, and \_\_\_\_\_, a  
\_\_\_\_\_.

1. Purpose. The parties wish to explore a business opportunity of mutual interest, and in connection with this opportunity, each party (the "disclosing party") may disclose to the other (the "receiving party") certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

2. "Confidential Information" means any information disclosed by either party to the other party, either directly or indirectly, in writing, orally or by inspection of tangible objects (including without limitation documents, prototypes, samples, plant and equipment), which is designated as "Confidential," "Proprietary" or some similar designation at or prior to the time of disclosure. Confidential Information shall include without limitation technical data, trade secrets and know-how, including, but not limited to, research, product plans, products, services, suppliers, customer lists and customer information, prices and costs, markets, software, developments, inventions, laboratory notebooks, processes, formulas, technology, designs, drawings, engineering, hardware configuration information, marketing, licenses, finances, budgets and other business information. Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which (i) was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party in violation of this Agreement; (iii) is already in the possession of the receiving party at the time of disclosure by the disclosing party as shown by the receiving party's files and records immediately prior to the time of disclosure; (iv) is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality; or (v) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by the receiving party's documents or other competent evidence in the receiving party's possession.

3. Non-use and Non-disclosure. Each party agrees not to use any Confidential Information of the other party for any purpose except to evaluate and engage in discussions concerning a potential business relationship between the parties. Each party agrees not to disclose any Confidential Information of the other party to third parties or to such party's employees, except to those employees of the receiving party who are required to have the information in order to evaluate or engage in discussions concerning the contemplated business relationship or to agents of a party retained to participate in licensing discussions between the parties.

4. Maintenance of Confidentiality. Each party shall ensure that its employees who have access to Confidential Information of the other party have signed a non-use and non-disclosure agreement in content substantially similar to the provisions hereof, prior to any disclosure of Confidential Information to such employees. Neither party shall make any copies of the Confidential Information of the other party unless the same are previously approved in writing by the other party. Each party shall reproduce the other party's proprietary rights notices on any such approved copies, in the same manner in which such notices were set forth in or on the original. If any material non-public information is disclosed, the recipient of such information agrees that it will comply with SEC Regulation FD (Fair Disclosure), and refrain from trading in the disclosing party's stock until that material non-public information is publicly disseminated. Notwithstanding anything to the contrary set forth herein, a receiving party shall be permitted to disclose Confidential Information to the extent (and only to the extent) the receiving party is required by law or upon advice of counsel to disclose such Confidential Information, provided that the receiving party gives the disclosing party prompt written notice of such requirement and upon the request of the disclosing party, the receiving party cooperates in good faith and at the expense of the disclosing party in any reasonable and lawful actions which the disclosing party takes to resist such disclosure or limit the information to be disclosed.

5. No Obligation. Nothing herein shall obligate either party to proceed with any transaction between them, and each party reserves the right, in its sole discretion, to terminate the discussions contemplated by this Agreement concerning the business opportunity.

6. No Warranty. ALL CONFIDENTIAL INFORMATION IS PROVIDED "AS IS". EACH PARTY MAKES NO WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, REGARDING ITS ACCURACY, COMPLETENESS OR PERFORMANCE.

7. Return of Materials. All documents and other tangible objects containing or representing Confidential Information which have been disclosed by either party to the other party, and all copies thereof which are in the possession of the other party, shall be and remain the property of the disclosing party and shall be promptly returned to the disclosing party or destroyed upon the termination of this Agreement or the disclosing party's written request. At the request of the disclosing party, the recipient will furnish a certificate, signed by an officer of the recipient, certifying that any Confidential Information not returned to the disclosing party has been destroyed.

8. No License. Nothing in this Agreement is intended to grant any rights to either party under any intellectual property rights of the other party, nor shall this Agreement grant any party any rights in or to the Confidential Information of the other party except as expressly set forth herein.

9. Term. The obligations of each receiving party hereunder shall survive for a period of five (5) years from the date of disclosure. Notwithstanding the expiration of the term, the obligations of Section 3 shall continue forever and shall terminate only at such time, and then only to the extent, the disclosing party's Confidential Information no longer constitutes Confidential Information.

10. Remedies. Each party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

11. Export. The parties acknowledge that the export of Confidential Information may be subject to regulations which may prohibit the export of such information to certain foreign countries or the disclosure of such information to certain foreign nationals. The parties, therefore, agree to comply strictly with all applicable export laws, regulations, executive orders and the like.

12. Miscellaneous. This Agreement shall bind and inure to the benefit of the parties hereto and their successors and assigns. This Agreement shall be governed by the laws of the State of Georgia, without reference to conflict of laws principles. This document contains the entire agreement between the parties with respect to the subject matter hereof, and neither party shall have any obligation, express or implied by law, with respect to trade secret or proprietary information of the other party except as set forth herein. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision. This Agreement may not be amended, nor any obligation waived, except by a writing signed by both parties hereto. This Agreement may be signed in counterparts, and delivered by facsimile, and such facsimile counterparts shall be valid and binding on the parties hereto with the same effect as if original signatures had been exchanged.

CommWorks Solutions, LLC

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

\_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

# Exhibit B

---

## KHEYFITS BELENKY LLP

TEL. (212) 203-5399  
FAX. (212) 203-6445

1140 AVENUE OF THE AMERICAS  
9TH FLOOR  
NEW YORK, NEW YORK 10036

WWW.KBLIT.COM

DMITRY KHEYFITS  
DKHEYFITS@KBLIT.COM

April 17, 2020

<b>By FedEx Ground (Tracking No. 770263257088) and email (Michael.Olsen@AlticeUSA.com)</b>  Michael Olsen Executive Vice President and General Counsel Altice USA, Inc. One Court Square Long Island City, New York 11101	
<b>By Priority Mail (Tracking No. 9405503699300333280949)</b>  General Counsel Suddenlink Communications 520 Maryville Centre Drive, Suite 300 St. Louis, Missouri 63141	<b>By Priority Mail (Tracking No. 9405503699300333301743)</b>  General Counsel CSC Holdings, LLC. 1111 Stewart Avenue Bethpage, New York 11714

Re: CommWorks Solutions, LLC

Dear Mr. Olsen:

By way of introduction, this law firm represents CommWorks Solutions, LLC (“CommWorks”) in connection with licensing of its patent portfolio. It is our understanding that you have already received a letter from CommWorks’ licensing agent, and I write to provide additional information. As previously noted by CommWorks, it owns over 140 U.S. Patents, which are listed in Exhibit A to this letter. Of particular interest to Altice USA, Inc. and its Optimum and Suddenlink branded services are the following patents (“CommWorks Patents”):

- U.S. Patent No. 6,832,249, entitled “Globally Accessible Computer Network-Based Broadband Communication System With User-Controllable Quality Of Information Delivery And Flow Priority” (“the ’249 Patent”);
- U.S. Patent No. 6,891,807, entitled “Time Based Wireless Access Provisioning” (“the ’807 Patent”);
- U.S. Patent No. 7,027,465, entitled “A Method For Contention Free Traffic Detection” (“the ’465 Patent”);
- U.S. Patent No. 7,177,285, entitled “Time Based Wireless Access Provisioning”

- (“the ’285 Patent”);
- U.S. Patent No. 7,463,596, entitled “Time Based Wireless Access Provisioning” (“the ’596 Patent”);
- U.S. Patent No. 7,760,664, entitled “Determining And Provisioning Paths In A Network” (“the ’664 Patent”);
- U.S. Patent No. 7,911,979, entitled “Time Based Access Provisioning System And Process” (“the ’979 Patent”);
- U.S. Patent No. 8,116,315, entitled “System And Method For Packet Classification” (“the ’315 Patent”);
- U.S. Patent No. RE44,904, entitled “A Method For Contention Free Traffic Detection” (“the ’904 Patent”).

Based on publicly available information, it is the understanding and contention of CommWorks that Altice USA, Inc. infringes and induces others, such as its customers, integrators, and suppliers, to infringe claims of the CommWorks Patents.

For example, Altice USA, Inc. infringes and induces others to infringe at least claim 17 of the ’807 Patent, claim 1 of the ’465 Patent, claim 1 of the ’285 Patent, claim 1 of the ’596 Patent, claim 19 of the ’979 Patent, and claim 7 of the ’904 Patent by making, using, offering for sale, selling, and/or importing into the United States Wi-Fi enabled modems and routers and Wi-Fi services.

Altice USA, Inc. also infringes and induces others to infringe at least claim 11 of the ’249 Patent by making, using, offering for sale, selling, and/or importing into the United States passive optical network (PON) equipment.

Altice USA, Inc. also infringes and induces others to infringe at least claim 7 of the ’315 Patent and claim 31 of the ’249 Patent by making, using, offering for sale, selling, and/or importing into the United States network switches and routers.

Altice USA, Inc. also infringes and induces others to infringe at least claim 7 of the ’664 Patent by making, using, offering for sale, selling, and/or importing into the United States network infrastructure provisioning tools used to provision network routers and switches.

Our purpose in writing to Altice USA, Inc. is to acquaint and/or reacquaint you with the CommWorks Patents, and to open a dialogue with you regarding a possible license under the CommWorks portfolio. Enclosed with this letter are copies of the CommWorks Patents.

Please note that CommWorks has not concluded analyzing the entirety of its assets, and it may reach out to you regarding infringement of additional patents. If you have any questions, please do not hesitate to contact me at the phone number or e-mail listed above.

Sincerely,

/s/ Dmitry Kheyfits

Dmitry Kheyfits

**Exhibit A****CommWorks Solutions, LLC Patents**

<b>Country</b>	<b>Patent No.</b>	<b>Title</b>
<b>US</b>	6335821	Optical Fiber Amplifier And A Method For Controlling The Same
<b>US</b>	6341221	Method Of Managing A Subscriber Service By An Intelligent Network Service
<b>US</b>	6427001	System And Method For Notification Of 911 Telephone Calls Using Link Monitoring System
<b>US</b>	6427037	Two-Stage Optical Switch Circuit Network
<b>US</b>	6433742	Diversity Antenna Structure For Wireless Communications
<b>US</b>	6438367	Transmission Security For Wireless Communications
<b>US</b>	6456242	Conformal Box Antenna
<b>US</b>	6456245	Card-Based Diversity Antenna Structure For Wireless Communications
<b>US</b>	6456764	Optical Directional Coupler
<b>US</b>	6483634	Optical Amplifier
<b>US</b>	6487406	PCS-To-Mobile IP Internetworking
<b>US</b>	6490067	Multi-Channel Optical Transceiver
<b>US</b>	6490259	Active Link Layer And Intra-Domain Mobility For IP Networks
<b>US</b>	6505163	Network And Method For Providing An Automatic Recall Telecommunications Service With Automatic Speech Recognition Capability
<b>US</b>	6594356	Initiating A Controlling Service
<b>US</b>	6621854	Spread-Spectrum Electromagnetic Signals
<b>US</b>	6628943	Mobility Management Utilizing Active Address Propagation
<b>US</b>	6636742	Tracking Of Mobile Terminal Equipment In A Mobile Communications System



Country	Patent No.	Title
US	6665495	Non-Blocking, Scalable Optical Router Architecture And Method For Routing Optical Traffic
US	6678080	Optical Add/Drop Multiplexer
US	6711122	Frequency Offset Differential Pulse Position Modulation
US	6721415	Telephone Voice Messaging System And Method Using Off-Hook Immediate Trigger
US	6721787	System And Method For Wireless Hot-Synchronization Of A Personal Digital Assistant
US	6724883	Processing Of Data Message In A Network Element Of A Communications Network
US	6748064	Systems And Methods For Least Cost Routing Of Long Distance Or International Telephone Calls
US	6754323	Establishing A Conference Call From A Call-Log
US	6754716	Restricting Communication Between Network Devices On A Common Network
US	6771971	Subscriber Information Service Center (SISC)
US	6775253	Adaptive Signaling For Wireless Packet Telephony
US	6775258	Apparatus, And Associated Method, For Routing Packet Data In An Ad Hoc, Wireless Communication System
US	6785534	Prepaid/Postpaid Automatic Change Of Payment Option
US	6788660	Adaptive Mobile Signaling For Wireless Internet Telephony
US	6792094	Intelligent Call Connection Service
US	6795530	System And Method For Customized Telephone Greeting Announcements
US	6804713	Operational Supervisory System For A Server
US	6832249	Globally Accessible Computer Network-Based Broadband Communication System With User-Controllable Quality Of Information Delivery And Flow Priority
US	6836466	Method And System For Measuring IP Performance Metrics
US	6857007	Personal Digital Assistant Facilitated Communication System
US	6859529	Method And System For Self-Service Scheduling Of Inbound Inquiries

<b>Country</b>	<b>Patent No.</b>	<b>Title</b>
<b>US</b>	6865237	Method And System For Digital Signal Transmission
<b>US</b>	6866587	Wide Area Real-Time Software Environment
<b>US</b>	6868268	Audio Calling Name And Number Delivery
<b>US</b>	6891807	Time Based Wireless Access Provisioning
<b>US</b>	6901437	Mobile Cache For Dynamically Composing User-Specific Information
<b>US</b>	6917605	Mobile Network System And Service Control Information Changing Method
<b>US</b>	6931003	Packet Prioritization Protocol For A Large-Scale, High Speed Computer Network
<b>US</b>	6956941	Method And System For Scheduling Inbound Inquiries
<b>US</b>	6967951	System For Reordering Sequenced Based Packets In A Switching Network
<b>US</b>	6975855	Method For Managing Mobile Station Facilities
<b>US</b>	6980089	Non-Intrusive Coupling To Shielded Power Cable
<b>US</b>	6985724	Device For Transmitting Data And Control Commands Via Radio Connections In A Distributed Control System For One Or More Machines And/Or Processes
<b>US</b>	7006579	ISI-Robust Slot Formats For Non-Orthogonal-Based Space-Time Block Codes
<b>US</b>	7023978	Telephone Voice Messaging System And Method Using Off-Hook Immediate Trigger
<b>US</b>	7027465	A Method For Contention Free Traffic Detection
<b>US</b>	7051116	Client Device Identification When Communicating Through A Network Address Translator Device
<b>US</b>	7061379	RFID System And Method For Ensuring Safety Of Hazardous Or Dangerous Substances
<b>US</b>	7062475	Personalized Multi-Service Computer Environment
<b>US</b>	7069483	System And Method For Identifying Nodes In A Wireless Mesh Network
<b>US</b>	7079823	Band-Pass Filter With Carrier Frequency Reduction
<b>US</b>	7092986	Transparent Mobile Ipv6 Agent

<b>Country</b>	<b>Patent No.</b>	<b>Title</b>
<b>US</b>	7106697	Method For Dynamically Computing A Switching Schedule
<b>US</b>	7124435	Information Management System And Method
<b>US</b>	7145867	System And Method For Slot Deflection Routing
<b>US</b>	7177285	Time Based Wireless Access Provisioning
<b>US</b>	7180850	Frequency Offset Differential Pulse Position Modulation
<b>US</b>	7184444	System And Method For Packet Classification
<b>US</b>	7190900	Non-Blocking All-Optical Switching Network Dynamic Data Scheduling System And Implementation Method
<b>US</b>	7206806	Method And System For Remote Utilizing A Mobile Device To Share Data Objects
<b>US</b>	7209950	Method And Apparatus For A Network Independent Short Message Delivery System
<b>US</b>	7218637	System For Switching Data Using Dynamic Scheduling
<b>US</b>	7224642	Wireless Sensor Data Processing Systems
<b>US</b>	7245201	Power Line Coupling Device And Method Of Using The Same
<b>US</b>	7248148	Power Line Coupling Device And Method Of Using The Same
<b>US</b>	7254709	Managed Information Transmission Of Electronic Items In A Network Environment
<b>US</b>	7355961	Method And Arrangement For Digital Signal Transmission Using Layered Space-Time Codes
<b>US</b>	7363030	Establishing A Conference Call From A Call-Log
<b>US</b>	7412514	Method And Apparatus For Improving Bandwidth Efficiency In A Computer Network
<b>US</b>	7443790	System And Method For Slot Deflection Routing At Optical Router/Switch
<b>US</b>	7451365	System And Method For Identifying Nodes In A Wireless Network
<b>US</b>	7460609	Transmission Method Using Complex Channel Symbols
<b>US</b>	7463596	Time Based Wireless Access Provisioning

Country	Patent No.	Title
US	7474853	Non-Blocking All-Optical Switching Network Dynamic Data Scheduling System And Implementation Method
US	7484005	Client Device Identification When Communicating Through A Network Address Translator Device
US	7496033	Method For Dynamically Computing A Switching Schedule
US	7526203	Apparatus And Method For Optical Switching At An Optical Switch Fabric
US	7555273	Bandpass Filter With Carrier Frequency Reduction
US	7564863	Frequency Offset Differential Pulse Position Modulation
US	7596533	Personalized Multi-Service Computer Environment
US	7609712	Frequency Offset Differential Pulse Position Modulation
US	7626918	Frequency Offset Differential Pulse Position Modulation
US	7715712	System And Method For Implementing Dynamic Scheduling Of Data In A Non-Blocking All-Optical Switching Network
US	7734807	Method And Apparatus For Improving Bandwidth Efficiency In A Computer Network
US	7760664	Determining And Provisioning Paths In A Network
US	7814230	Client Device Identification When Communicating Through A Network Address Translator Device
US	7835350	Prioritizing Data Transmissions Using The Number Of Associated Origin Addresses
US	7835372	System And Method For Transparent Wireless Bridging Of Communication Channel Segments
US	7835897	Apparatus And Method For Connecting Hardware To A Circuit Simulation
US	7852796	Distributed Multichannel Wireless Communication
US	7856011	Reordering Packets
US	7869427	System For Switching Data Using Dynamic Scheduling
US	7911979	Time Based Access Provisioning System And Process
US	7937081	Recovery Techniques In Mobile Networks

Country	Patent No.	Title
US	7941149	Multi-Hop Ultra Wide Band Wireless Network Communication
US	7957356	Scalable Media Access Control For Multi-Hop High Bandwidth Communications
US	8031800	Transmitting Digital Signal
US	8107377	Reordering Packets
US	8116315	System And Method For Packet Classification
US	8117068	Method And Apparatus For Providing Audio Advertisements In A Computer Network
US	8160863	System And Method For Connecting A Logic Circuit Simulation To A Network
US	8175613	Systems And Methods For Determining Location Of Devices Within A Wireless Network
US	8195442	Use Of Hardware Peripheral Devices With Software Simulations
US	8200211	Recovery Techniques In Mobile Networks
US	8224909	Personal Digital Assistant Facilitated Communication System
US	8351924	Recovery Techniques In Mobile Networks
US	8380481	Conveying Data From A Hardware Device To A Circuit Simulation
US	8423630	Responding To Quality Of Service Events In A Multi-Layered Communication System
US	8533278	Mobile Computing Device Based Communication Systems And Methods
US	8600372	Recovery Techniques In Mobile Networks
US	8611320	Scalable Media Access Control For Multi-Hop High Bandwidth Communications
US	8671216	Method And Apparatus For Improving Bandwidth Efficiency In A Computer Network
US	8719326	Adaptive Data Transformation Engine
US	8780770	Systems And Methods For Voice And Video Communication Over A Wireless Network
US	8812665	Globally Accessible Computer Network-Based Broadband Communication System With User-Controllable Quality Of Information Delivery And Flow Priority

<b>Country</b>	<b>Patent No.</b>	<b>Title</b>
<b>US</b>	8913618	Reordering Packets
<b>US</b>	8923846	Recovery Techniques In Mobile Networks
<b>US</b>	9230039	Adaptive Data Transformation Engine
<b>US</b>	9432842	Recovery Techniques In Mobile Networks
<b>US</b>	9554304	Scalable Media Access Control For Multi-Hop High Bandwidth Communications
<b>US</b>	9648122	Mobile Cache For Dynamically Composing User-Specific Information
<b>US</b>	9918222	Recovery Techniques In Mobile Networks
<b>US</b>	9930575	Scalable Media Access Control For Multi-Hop High Bandwidth Communications
<b>US</b>	10051077	Mobile Cache For Dynamically Composing User-Specific Information
<b>US</b>	RE42122	System And Method For Customized Telephone Greeting Announcements
<b>US</b>	RE42227	Apparatus And Method For Connecting Hardware To A Circuit Simulation
<b>US</b>	RE42232	RF Chipset Architecture
<b>US</b>	RE42539	Network And Method For Providing A Calling Name Telecommunications Service With Automatic Speech Recognition Capability
<b>US</b>	RE42883	Enhanced Phone-Based Collaboration
<b>US</b>	RE43163	High-Speed Network Of Independently Linked Nodes
<b>US</b>	RE43704	Determining And Provisioning Paths Within A Network Of Communication Elements
<b>US</b>	RE43746	Method And Radio System For Digital Signal Transmission Using Complex Space-Time Codes
<b>US</b>	RE44904	A Method For Contention Free Traffic Detection



# Exhibit C

---



Day Building, Suite 230  
4725 Peachtree Corners Circle,  
Peachtree Corners, GA 30092

Main: (404) 962-8740  
Fax: (404) 962-8741

[www.ipigrp.com](http://www.ipigrp.com)

May 15, 2020

VIA EMAIL / FEDEX

Rebecca Baneman  
Vice President, Legal – Litigation  
Altice USA, Inc.  
One Court Square  
Long Island City, New York 11101

**RE: COMMWORKS SOLUTIONS, LLC (“COMMWORKS”) - PATENT PORTFOLIO  
LICENSING PROGRAM**

Dear Ms. Baneman:

To follow up on our previous communications between CommWorks and Altice, and Kheyfits Belenky’s letter on behalf of CommWorks to Altice on April 17, 2020 (see attached), CommWorks would like to bring several additional patents to your attention. The following CommWorks patents relate to the Altice Mobile phone service:

- U.S. Patent No. 6,341,221, entitled “Method Of Managing A Subscriber Service By An Intelligent Network Service” (“the ’221 Patent”);
- U.S. Patent No. 6,594,356, entitled “Initiating A Controlling Service” (“the ’356 Patent”);
- U.S. Patent No. 6,636,742, entitled “Tracking Of Mobile Terminal Equipment In A Mobile Communications System” (“the ’742 Patent”);
- U.S. Patent No. 6,917,605, entitled “Mobile Network System And Service Control Information Changing Method” (“the ’605 Patent”);
- U.S. Patent No. 6,975,855, entitled “Method For Managing Mobile Station Facilities” (“the ’855 Patent”);
- U.S. Patent No. 7,209,950, entitled “Method And Apparatus For A Network Independent Short Message Delivery System” (“the ’950 Patent”);
- U.S. Patent No. 7,937,081, entitled “Recovery Techniques in Mobile Networks” (“the ’081 Patent”);
- U.S. Patent No. 8,200,211, entitled “Recovery Techniques in Mobile Networks” (“the ’211 Patent”);



Ms. Rebecca Baneman  
May 15, 2020  
Page 2

---

- U.S. Patent No. 8,600,372, entitled “Recovery Techniques In Mobile Networks” (“the ’372 Patent”);
- U.S. Patent No. 8,923,846, entitled “Recovery Techniques In Mobile Networks” (“the ’846 Patent”);
- U.S. Patent No. 9,918,222, entitled “Recovery Techniques In Mobile Networks” (“the ’222 Patent”);
- U.S. Patent No. RE42,883, entitled “Enhanced Phone-Based Collaboration” (“the ’883 Patent”).

Based on publicly available information, it is the understanding and contention of CommWorks that Altice infringes and induces others, such as its customers, integrators, and suppliers, to infringe claims of the above CommWorks patents.

For example, Altice infringes and induces others to infringe at least claim 1 of the ’221 Patent (*see* 3GPP TS 23.082 V6.0.0 (2004-12)), claim 1 of the ’356 Patent (*see* 3GPP TS 29.078 7.0.0 (2005-06); 3GPP2 X.S0004-700-E v1.0 (2004-03)), claim 1 of the ’742 Patent (*see* 3GPP TS 23.171 V3.11.0 (2004-03); 3GPP2 X.S0002-0 v2.0 (2006-05)), claim 16 of the ’605 Patent (*see* 3GPP TS 29.061 V6.0.0 (2004-03)), and claim 1 of the ’855 Patent (*see* 3GPP TS 23.097 V6.0.0 (2004-12)) by making, using, offering for sale, selling, and/or importing into the United States GSM/UMTS and/or CDMA2000 compliant features of the Altice mobile services.

Altice also infringes and induces others to infringe at least claim 1 of the ’950 Patent by making, using, offering for sale, selling, and/or importing into the United States GSMA compliant SMS Hubbing features of the Altice mobile services.

Altice also infringes and induces others to infringe at least claim 1 of the ’081 Patent, claim 1 of the ’211 Patent, claim 1 of the ’372 Patent, claim 1 of the ’846 Patent, and claim 1 of the ’222 Patent, by making, using, offering for sale, selling, and/or importing into the United States LTE compatible Altice mobile networking systems and services, including its IP Multimedia Subsystem infrastructure.

Altice also infringes and induces others to infringe at least claim 1 of the ’883 Patent by making, using, offering for sale, selling, and/or importing into the United States VoLTE compatible Altice mobile systems and services.



Ms. Rebecca Baneman  
May 15, 2020  
Page 3

---

As mentioned previously, CommWorks welcomes a discussion with Altice with respect to a potential license to the CommWorks patent portfolio. Once you have had sufficient time to review the information CommWorks has presented, please let me know if Altice is interested in discussing a resolution to this matter.

Sincerely,

  
\_\_\_\_\_  
Ryan E. Strong

cc: Dmitry Kheyfits, Esq., Kheyfits Belenky, LLP

Enclosures

# Exhibit D

---

919 THIRD AVENUE NEW YORK, NY 10022-3908

JENNER & BLOCK LLP

June 3, 2020

Amr O. Aly  
Tel +1 212 407 1774  
AAly@jenner.com

Mr. Ryan E. Strong  
IPinvestments Group  
Day Building, Suite 230  
4725 Peach Corners Circle  
Peachtree, GA 30092

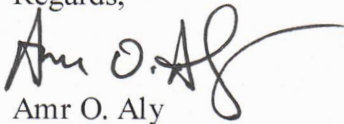
Re: **COMM WORKS SOLUTIONS, LLC ("COMMWORKS") -  
PATENT PORTFOLIO LICENSING PROGRAM**

Dear Mr. Strong:

I represent Altice USA and am in receipt of your letters dated February 21, 2020, and May 15, 2020 both addressed to Ms. Rebecca Baneman. Altice USA respects intellectual property rights of others, and is evaluating your claims of patent infringement of certain patents owned by CommWorks Solutions, LLC. To the extent you have additional information that would aid in our analysis, such as infringement charts, we would appreciate receiving same.

In the meantime, please do not hesitate to contact me if you have any questions.

Regards,

  
Amr O. Aly

AOA:mr

# Exhibit E

---





US006832249B2

(12) **United States Patent**  
**Ciscon et al.**

(10) **Patent No.:** **US 6,832,249 B2**  
(45) **Date of Patent:** **Dec. 14, 2004**

(54) **GLOBALLY ACCESSIBLE COMPUTER NETWORK-BASED BROADBAND COMMUNICATION SYSTEM WITH USER-CONTROLLABLE QUALITY OF INFORMATION DELIVERY AND FLOW PRIORITY**

(75) Inventors: **Larry Ciscon**, Houston, TX (US);  
**Steven Reynolds**, Houston, TX (US); **F. Scott Yeager**, Sugarland, TX (US)

(73) Assignee: **Intellectual Ventures Patent Holdings III, LLC**, Bellevue, WA (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 719 days.

(21) Appl. No.: **09/860,801**

(22) Filed: **May 18, 2001**

(65) **Prior Publication Data**

US 2002/0004827 A1 Jan. 10, 2002

#### **Related U.S. Application Data**

(60) Provisional application No. 60/205,529, filed on May 19, 2000.

(51) **Int. Cl.**<sup>7</sup> ..... **G06F 13/00**

(52) **U.S. Cl.** ..... **709/223**

(58) **Field of Search** ..... 709/200, 223;  
370/328, 338, 903

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

6,747,968 B1 \* 6/2004 Seppala et al. .... 370/338

\* cited by examiner

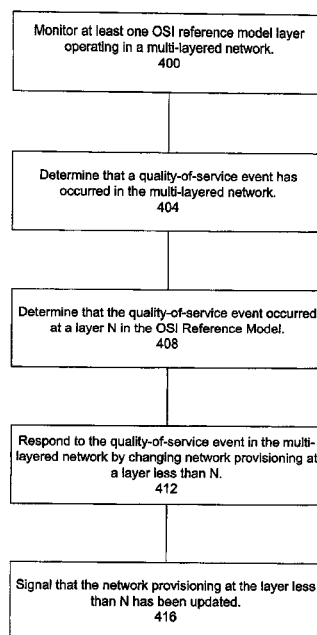
*Primary Examiner*—Robert B. Harrell

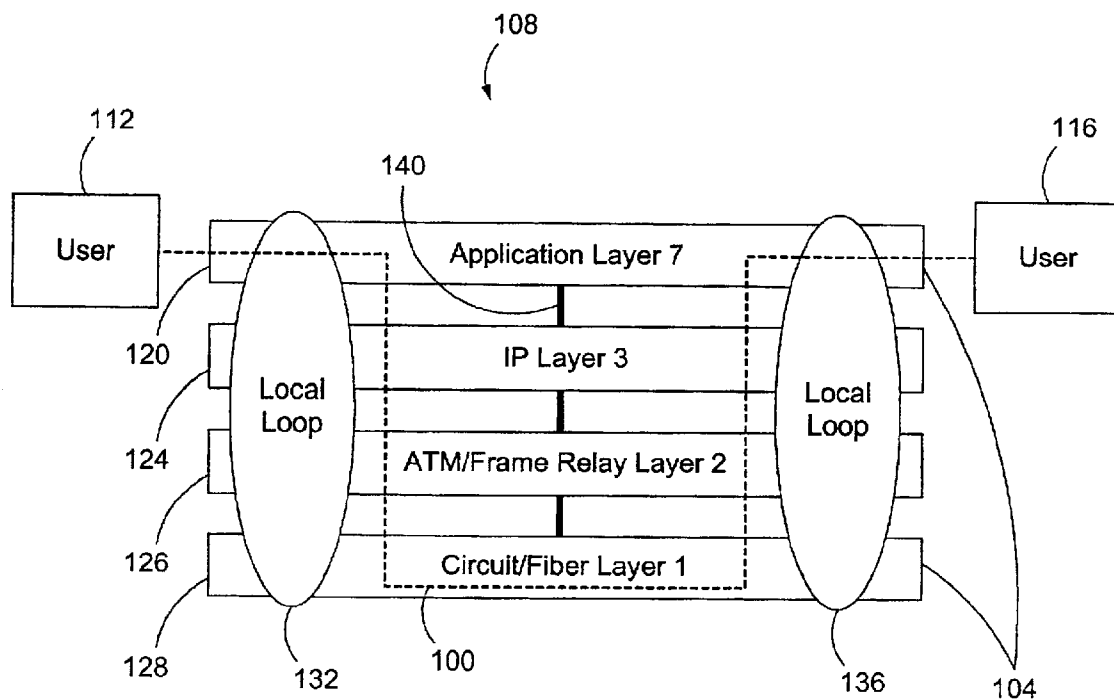
(74) *Attorney, Agent, or Firm*—Wong, Cabello, Lutsch, Rutherford & Brucculeri, LLP

(57) **ABSTRACT**

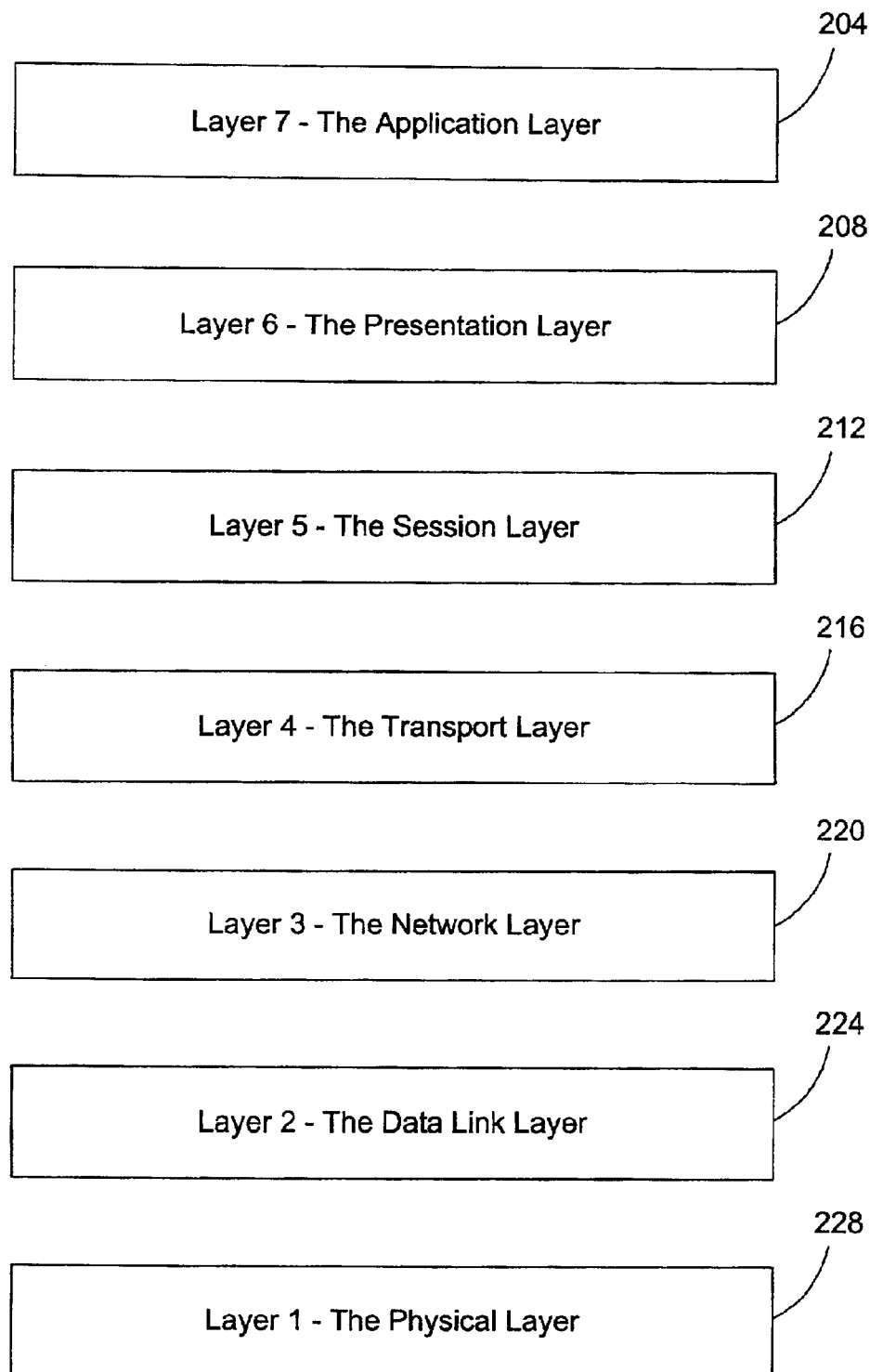
A method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) Reference Model layers functioning therein includes monitoring at least one OSI reference model layer functioning in the multi-layered network. A quality of service event is determined whether to have occurred in the multi-layered network. The quality of service event is determined to have occurred at a layer N in the OSI reference model. Network provisioning is changed at a layer less than N in response to the quality of service event, and a signal is provided when the network provisioning at the layer less than N has been changed. A system for providing broadband communications includes a multi-layered network, a network monitor, and a network controller. The multi-layered network has a plurality of Open System Interconnection (OSI) reference model layers functioning therein. The network monitor is coupled to the multi-layered network, and the network monitor is adapted to monitor at least one OSI reference model layer functioning in the multi-layered network, determine that a quality of service event has occurred in the multi-layer network, and determine that the quality of service event occurred at a layer N in the OSI reference model. The network controller is coupled to the multi-layered network, and the network monitor is adapted to respond to the quality of service event in the multi-layered network by changing the network provisioning at a layer less than N.

**49 Claims, 8 Drawing Sheets**

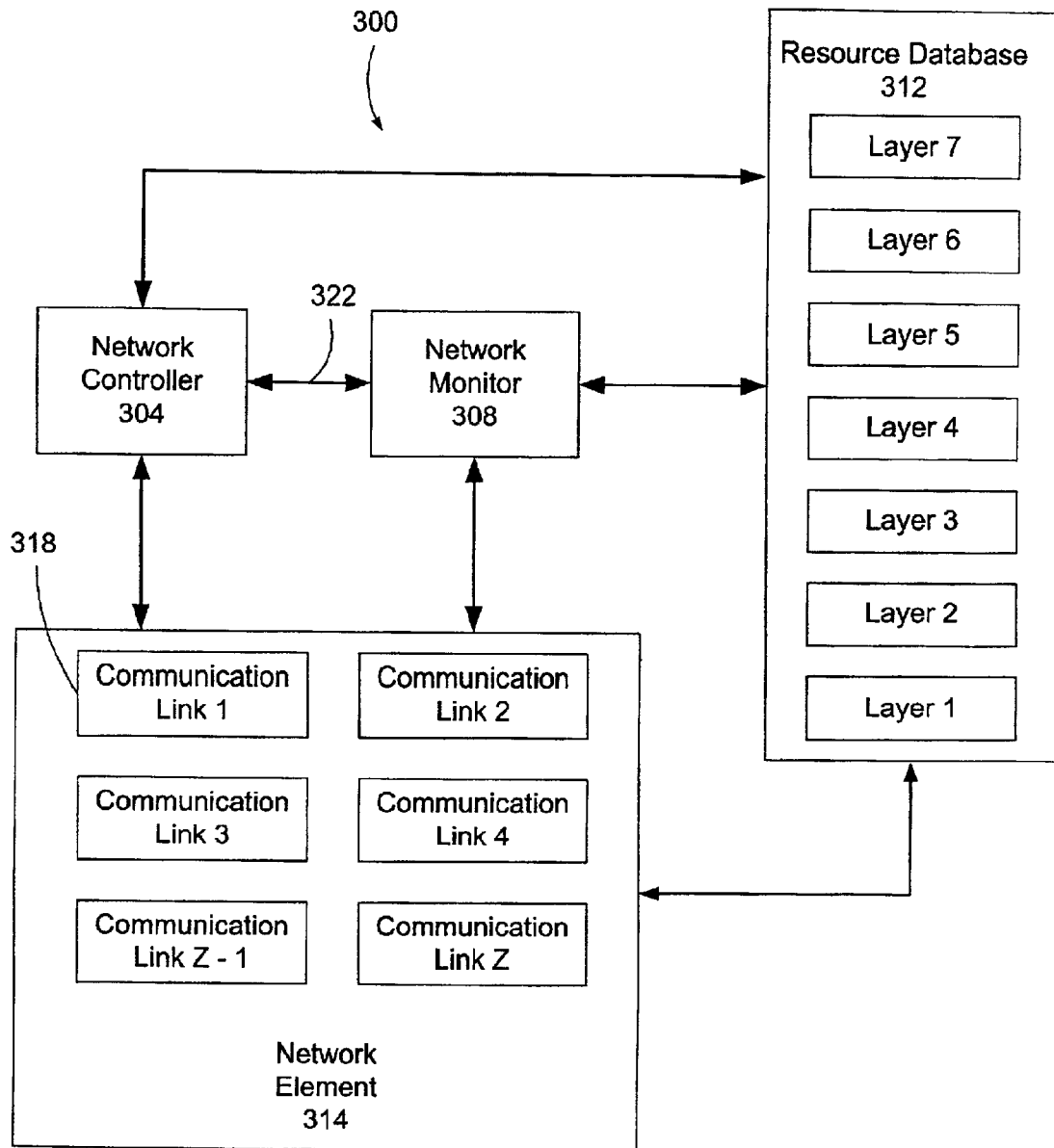


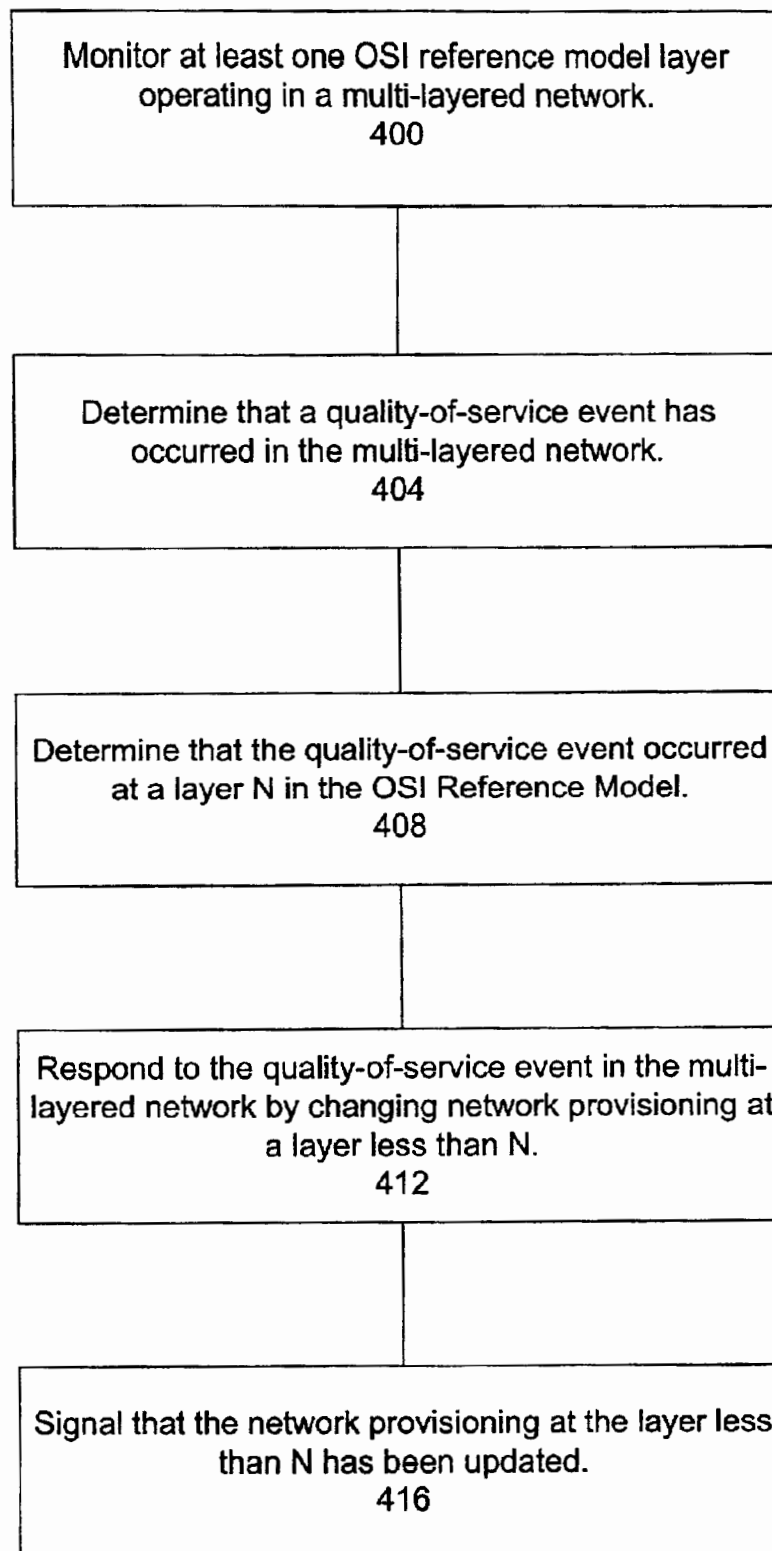


**Figure 1**  
**(Prior Art)**



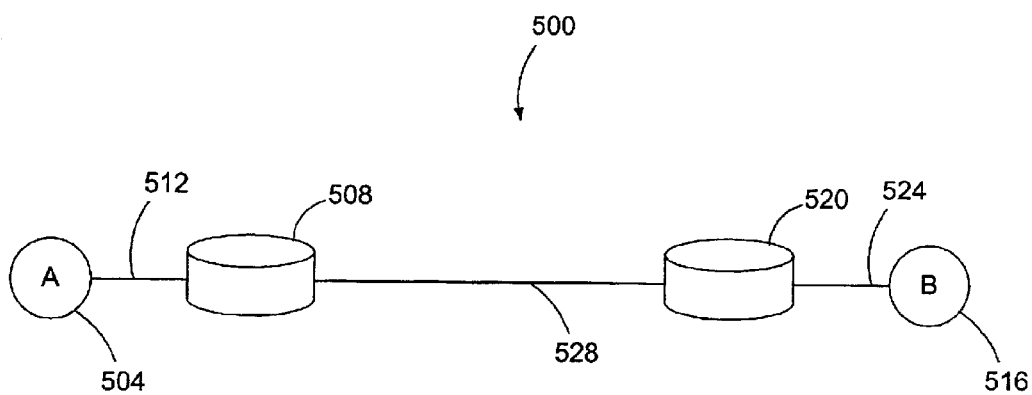
**Figure 2**  
**(Prior Art)**

**Figure 3**

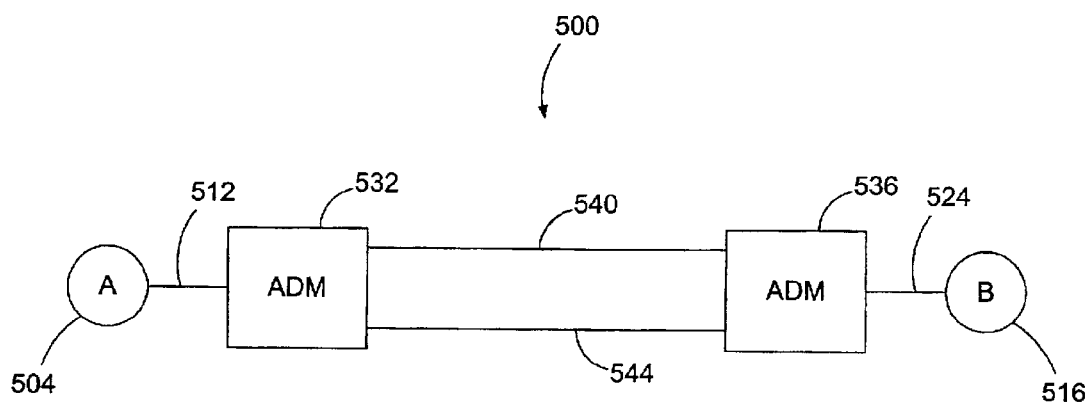


**Figure 4**





**Figure 5A**



**Figure 5B**

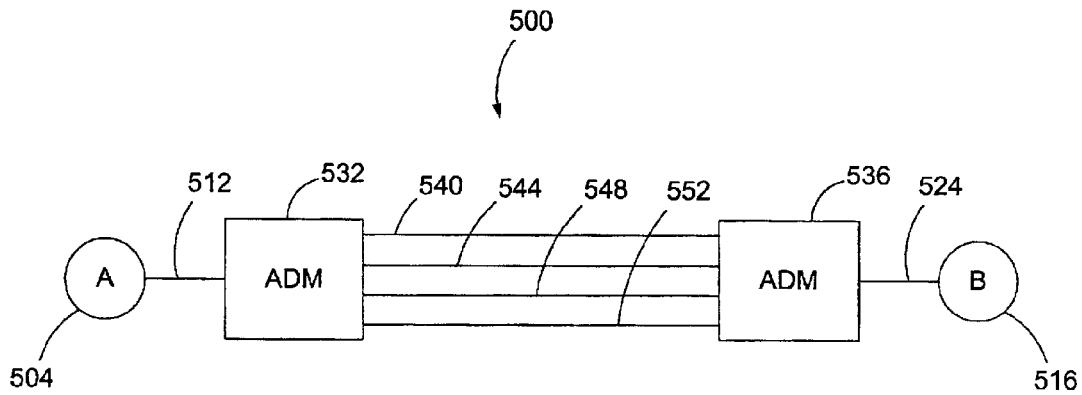


Figure 5C

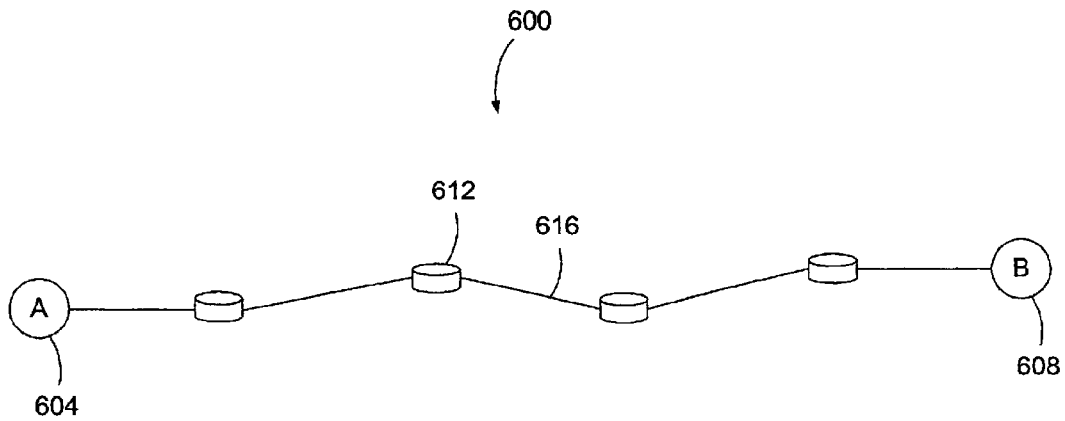


Figure 6A

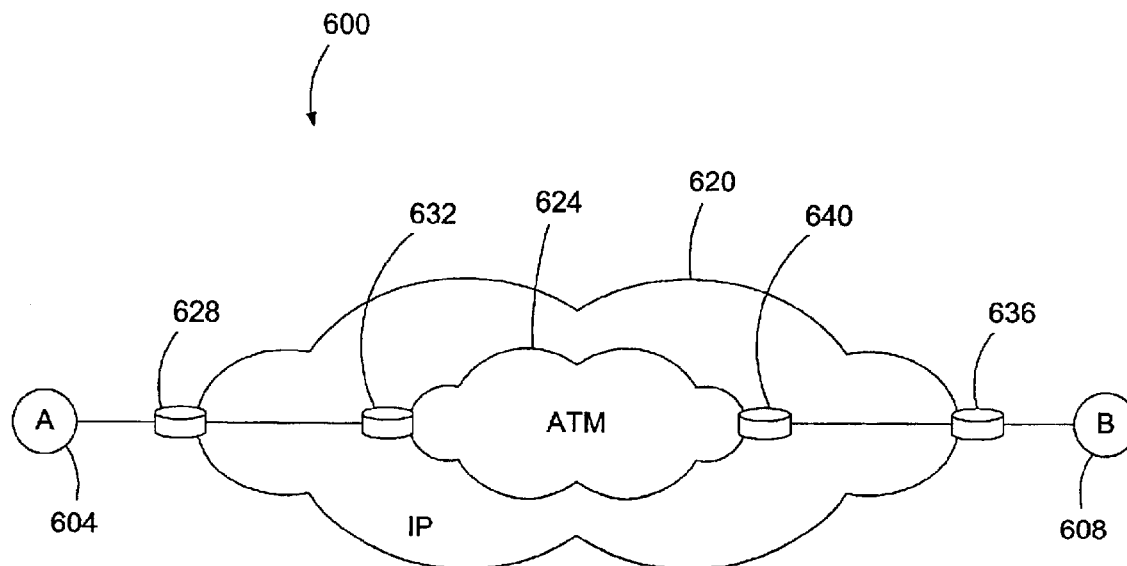


Figure 6B

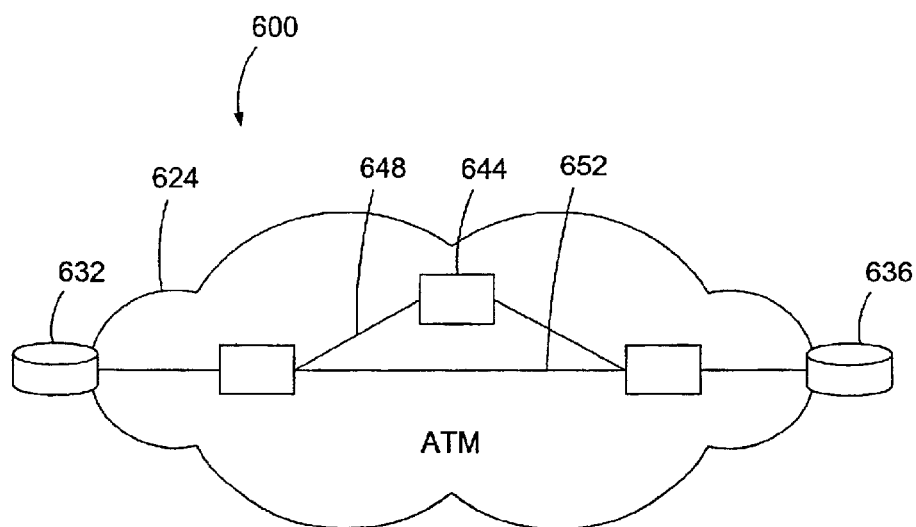
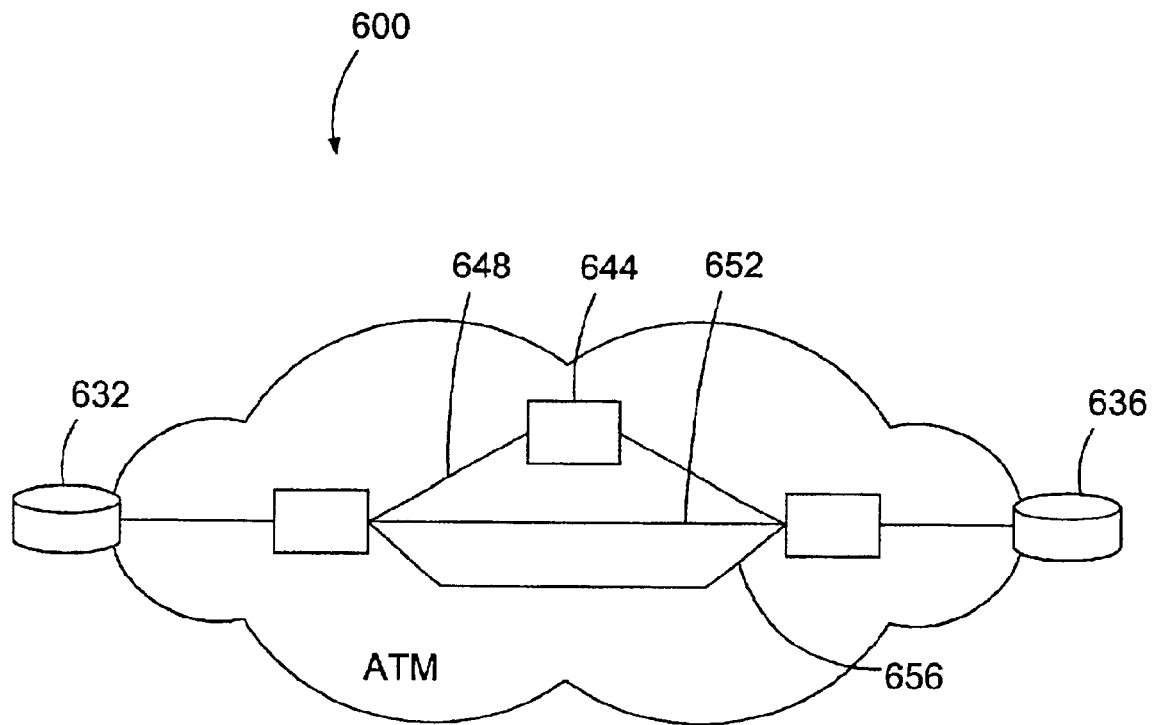


Figure 6C



**Figure 6D**

US 6,832,249 B2

1

**GLOBALLY ACCESSIBLE COMPUTER  
NETWORK-BASED BROADBAND  
COMMUNICATION SYSTEM WITH  
USER-CONTROLLABLE QUALITY OF  
INFORMATION DELIVERY AND FLOW  
PRIORITY**

This application claims the benefit of U.S. Provisional Application No. 60/205,529 filed May 19, 2000.

**BACKGROUND OF THE INVENTION**

**1. Field of the Invention**

The present invention relates generally to a communication system that operates in association with a globally accessible computer network, such as the Internet, and, more particularly, to a multi-layered communication system that is implemented with a broadband communications platform that enables quality of application service delivery and user control over the priority of information delivery flow.

**2. Description of the Related Art**

The Internet has become vital to both businesses and consumers. The initial role of the Internet as an information tool has led to explosive adoption of its use; however, the massive growth of the Internet has outpaced the capabilities of its infrastructure. Content providers have moved from providing static information to distributing applications that consume large amounts of bandwidth.

The delivery of high quality service to an end user while maintaining an ability to provide a significant increase in bandwidth over a global reach is an unmet challenge of contemporary communication systems. The public Internet is plagued with user problems such as congestion (too many users) and latency (long pauses and delays) and is, therefore, unable to support an increase in communication network traffic resulting from the presence of additional users and the advent of rich media applications. Deterministic applications include, for example, media rich content, low latency applications, and other applications requiring mission critical delivery scheduling. Several causes of user problems are deliberate off-loading and routing of data traffic through congestion points, inadequate security, and lost information resulting from the currently used best-effort routing practices.

The structural layers of the Internet, which include network providers, service providers, software providers, and content providers, work independently and thereby create an infrastructure based on individual convenience and legacy systems without consideration of the interaction among the constituent participants. Telecommunication carriers have networks optimized for voice but not data. Internet Service Providers (ISPs) oversubscribe their networks in an effort to achieve or sustain profitability. The public Internet is, therefore, a fundamentally flawed model from a financial, business, and technological perspective for the delivery of low latency, high throughput applications, such as media rich content and other deterministic applications.

Moreover, the Internet has a different set of transmission issues from those faced by Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs). LANs include directories that authorize LAN end-users to use applications or obtain information. The directory is a baseline component of the functionality that comes with LAN connectivity. LANs have historically been more important to businesses than residences because LANs enable enterprise-wide applications. MANs facilitate the interconnection of corporate LANs between buildings in

2

a city as well as enable the interconnection of corporate networks to a WAN for voice and data traffic. They are also the local loop infrastructure that connects end users to the Internet. WANs serve as the backbone for corporations that operate in multiple cities and are the national or global networks that connect the majority of users. Public WANs, which serve as the Internet backbone, have large amounts of available bandwidth; however, no widely used routing system exists that avoids the congestion and best efforts delivery method of today's Internet.

The Internet at numerous points has congestion that results from "peering" and commercially expedient routing policies at the peering points, such as Metropolitan Area Exchanges (MAEs), where there is no economic incentive to carry traffic over any particular equipment backbone structure. Peering routing is a consequence of the practice of multiple service providers (SPs) using their routers to exchange information transmission routes with one another. Commercially expedient routing is the practice of an SP choosing a nearest location to transfer applications, irrespective of quality of service considerations. Thus, the finite number of available locations for exchanging information becomes overly congested because application routing is motivated by commercial, not quality of service control, considerations.

The Internet operates with end users by way up dial-up modems or LANs connected by an ISP local loop and thereby create over the LAN a load that typically exceeds the speed capability of the local loop. The consequence is that simple, high capacity bandwidth within the Internet by way of any ISP of rudimentary quality of service is insufficient to create a low latency, deterministic network solution. The demands exerted on infrastructure support required by, for example, 10 million users simultaneously on line from all branches of the Internet currently present a difficult bandwidth load management challenge, which promises to worsen as broadband applications gain popularity and increase in usage.

What is needed, therefore, is a broadband communication system that can consistently deliver deterministic applications, irrespective of network-to-network architecture complications.

The present invention is directed to overcoming, or at least reducing the effects of, one or more of the problems set forth above.

**SUMMARY OF THE INVENTION**

In one aspect of the present invention, a method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) Reference Model layers functioning therein is provided. The method includes monitoring at least one OSI reference model layer functioning in the multi-layered network. A quality of service event is determined whether to have occurred in the multi-layered network. The quality of service event is determined to have occurred at a layer N in the OSI reference model. Network provisioning is changed at a layer less than N in response to the quality of service event, and a signal is provided when the network provisioning at the layer less than N has been changed.

In another aspect of the present invention, a system is provided. The system includes a multi-layered network, a network monitor, and a network controller. The multi-layered network has a plurality of Open System Interconnection (OSI) reference model layers functioning therein. The network monitor is coupled to the multi-layered



US 6,832,249 B2

3

network, and the network monitor is adapted to monitor at least one OSI reference model layer functioning in the multi-layered network, determine that a quality of service event has occurred in the multi-layer network, and determine that the quality of service event occurred at a layer N in the OSI reference model. The network controller is coupled to the multi-layered network, and the network monitor is adapted to respond to the quality of service event in the multi-layered network by changing the network provisioning at a layer less than N.

### BRIEF DESCRIPTION OF THE DRAWINGS

The invention may be best understood by reference to the following description taken in conjunction with the accompanying drawings, in which like reference numerals identify like elements, and in which:

FIG. 1 illustrates a simplified prior art communication system;

FIG. 2 illustrates the functional layers of the Open System Interconnection (OSI) reference model;

FIG. 3 is a simplified block diagram of an illustrative network control system;

FIG. 4 is a simplified block diagram illustrating one exemplary process for the network control system, illustrated in FIG. 3, in accordance with one aspect of the present invention;

FIGS. 5A–5C illustrate an exemplary communication system when viewed from different levels of the OSI reference model;

FIGS. 6A–6D illustrate another exemplary communication system when viewed from different levels of the OSI reference model.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and are herein described in detail. It should be understood, however, that the description herein of specific embodiments is not intended to limit the invention to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

### DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

Illustrative embodiments of the invention are described below. In the interest of clarity, not all features of an actual implementation are described in this specification. It will of course be appreciated that in the development of any such actual embodiment, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which will vary from one implementation to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking for those of ordinary skill in the art having the benefit of this disclosure.

The broadband communication services delivery afforded by the present invention enables quality of service control by content providers, Application Service Providers (ASPs), local loop carriers, ISPs, and, by extension, their customers. This is achieved through a quality of service-capable broadband system that augments the Internet. The result is more control by users over the priority of their information flow, more control by network administrators over the congestion

4

of their networks, and more control by content providers over costs and the experiences they provide to their users.

Referring to FIG. 1, a prior art application data flow path **100** through functional layers **104** of a communication system **108**, such as the Internet, is shown. The basis of the functional layers **104** is the Open System Interconnection (OSI) model. In this model, information may be communicated between first and second users **112**, **116** by traversing through the functional layers **104** as shown.

Referring to FIG. 2, an illustrative block diagram **200** of the OSI reference model is shown. Those skilled in the art will appreciate that the OSI reference model is comprised of seven separate layers (four of which are illustrated in FIG. 1.) The seven layers of the OSI model include an application layer **204**, a presentation layer **208**, a session layer **212**, a transport layer **216**, a network layer **220**, a data link layer **224**, and a physical layer **228**. This model provides a useful reference when describing the various functions that may be involved in sending data across any communication system, such as the Internet. Moreover, those skilled in the art will appreciate that sending data across a communication system may require traversing any number of the functional layers of the OSI reference model. Furthermore, it may be appreciated that the communication resources (e.g., network devices, programs, protocols, hardware, software, etc.) in a multi-layered communication system may be described, at least in part, by where they fit in the OSI reference model.

The physical layer **228** is layer **1** in the OSI reference model. This layer encompasses the physical features of sending data over communication lines. For example, layer **1** may be associated with coaxial cables, fiber lines, category 1–5 cables, and the like.

The data link layer **224** is layer **2** in the OSI reference model. This layer encompasses procedures concentrated on the operation of communication lines. Error identification and correction are also functions of this layer. Layer **2** may include SLIP, PPP, Ethernet, and the like.

The network layer **220** is layer **3** in the OSI reference model. This layer establishes how data is transmitted between workstations, including the routing of data. Layer **3** may include IPV6, IPV4, and the like.

The transport layer **216** is layer **4** in the OSI reference model. This layer directs the processes for end-to-end transfer of information inside and between networks, including error recovery and flow control. Layer **4** may include TCP, UDP, and the like.

The session layer **212** is layer **5** in the OSI reference model. The layer controls communication resources and manages dialogue and the directions of information flow. Layer **5** may include POP/25, 532, RPC Portmapper, and the like.

The presentation layer **208** is layer **6** in the OSI reference model. This layer allows different systems to communicate by converting the information format of an individual system into a standard configuration. Layer **6** may include HTTP, FTP, SMTP, and the like.

The application layer **204** is layer **7** in the OSI reference model. This layer includes protocols for specific application services and encloses virtual terminal software. File transfer may also occur with events at the application layer. Layer **7** may include e-mail, newsgroups, web applications, and the like.

Although illustrative examples have been given for each of the **7** layers in the OSI reference model, those skilled in the art will appreciate that many other communication

US 6,832,249 B2

5

resources may be categorized by where their functionality fits within the OSI reference model. Moreover, some communication resources may not fit completely within one layer of the OSI reference model, that is, the functionality of some communication resources may be best categorized with reference to more than one OSI reference model layer. Nevertheless, most communication resources (e.g., routers, multiplexers, switches, data lines, application programs, software, hardware, etc.) may be substantially categorized within one of the layers of the OSI reference model.

For the ease of illustrating the present invention, the layers of the OSI reference model may be expressed algebraically. For example, layer 3, the network layer 220, may be described illustratively as layer N. If this is the case, then the layer N-1 would be layer 2, the data link layer 224, and the layer N-2 would be layer 1, the physical layer 228. Similarly, if layer 3 is again expressed as layer N, then the layers less than N would be comprised of layer 2 and layer 1. In another example, if layer 7, the application layer 204, is described illustratively as layer N, then the layer N-1 would be layer 6, the presentation layer 208. Likewise, if layer 7 is described as layer N, then the layers less than N would include layers 6 through 1.

Referring back to FIG. 1, the data flow path 100 is shown traversing 4 of the OSI functional layers 104. These layers include the application layer 120 (layer 7), the network layer 124 (layer 3), the data link layer 126 (layer 2), and the physical layer 128 (layer 1.) Those skilled in the art will appreciate that the data path 100 does not necessarily have to flow through all 7 of the OSI layers, illustrated in FIG. 2, in order to facilitate a communication session between the first and second users 112, 116. Rather, the OSI layers traversed by the data flow path 100 may vary depending upon a variety of factors, such as the type of connection between the first and second users 112, 116, the topology of the communication link between the first and second users 112, 116, the geographic location of the first and second users 112, 116, the particular application sending the data, and the like.

As described above, if the OSI layers 104 are expressed algebraically, in this example, layer 7 may be considered layer N, while the layers less than N may be the network layer 124 (layer 3), the data link layer 126 (layer 2), and the physical layer 128 (layer 1.) Similarly, layer 3 could be considered layer N, which would make the layers less than N the data link layer 126 (layer 2) and the physical layer 128 (layer 1.)

In this illustrative embodiment, each of the OSI reference model layers 104 may be implemented with an independent control system that operates under either central or distributed control. For example, the physical layer 128 (layer 1) may represent the provision of circuits that effects an end-to-end connection between the first and second users 112, 116 with an associated bandwidth, irrespective of the type of data or nature of the protocol. In the case of fiber optic cable, there may be multiple light transmissions wavelengths that provide separate information transmission channels. Carrier signal modulation and wavelength division multiplexing may also be carried out in layer 1. Layer 1 typically operates under control of a single computer that sends control signals to all devices in the layer.

The network layer 124 (layer 3) may operate internally as a distributed IP layer under dynamic routing protocols in the absence of a centralized computer. The application layer 120 (layer 7) may be a web browser sending HTTP protocol.

Additionally, the first user 112 may be connected to a first local loop 132, and the second user 116 may be connected

6

to a second local loop 136. The local loops 132, 136 may be comprised of LANs that connect the first and second users 112, 116 to the Internet. Although FIG. 1 is being described with reference to the Internet, it is contemplated that other communication systems (e.g., private Intranets, leased lines, etc.) may be used to send data between the first and second users 112, 116.

The backbone services, which are represented by line 140, represent a WAN of multiple geographically distributed locations, the equipment of which implement segmented connectivity through the Internet. For example, each location may operate equipment under an internal switching scheme that moves locally the transmitted information up and down the OSI layers. The WAN, therefore, may represent a network implementing a geographical progression of information transmitted up and down local OSI layers, such as the OSI layers 104 illustrated in FIG. 1.

Internet users define their services offered in terms of the functional layers of the OSI model and accordingly dictate business strategies. With reference again to FIG. 1, as applications/content are sent between the first and second users 112, 116, the applications/content traverse each of the illustrated OSI layers 104 to travel from end to end of the communication system 108. Service offerings such as private communication lines (circuits) or dark fiber may be available at Layer 1, so that an application developer must determine how to make the application function with TCP/IP, and a network architect for each application and project may determine whether to use ATM or Frame Relay transmission. The product managers of the individual services, circuits, fiber, ATM, Frame Relay, or IPS services may define the particular service at the corresponding layer 104. Of course, much of this interaction occurs transparently to the first and second users 112, 116.

The carrier service at an OSI reference layer is, typically, concerned only with how the end user or enterprise connects into its network at the correct points of demarcation on the network of the carrier service at that layer. There is usually no consideration of making the application work end-to-end up and down the OSI model stack 104 in any of these carrier class services.

As a practical matter, no single OSI reference layer can resolve all of the quality of service and economic issues associated with delivering deterministic applications such as streaming media content across the local loops 132, 136 and the backbone 140 between the users 112, 116 by way of networks of multiple service providers. The application traverses up and down the OSI stack 104 and may need quality of service functions at several layers to achieve end-to-end quality of service at a price that is economical for connecting a target audience.

Typically, the applications/content source needs to use more than one service (e.g., communication circuits, ATM and Frame Relay transmission technologies) from more than one OSI layer 104 to make the application reach all of the intended audiences that are dispersed geographically in different cities and countries across the world. No consistent policy exists to ensure quality of service in this approach.

The present invention implements a different approach to the typical Internet model. The strategy of the present invention is to bridge the gaps between the layers of the OSI reference model, illustrated in FIG. 2.

Referring to FIG. 3, an exemplary network control system 300 (control system) is shown. In this illustrative embodiment, the control system 300 may be comprised of a network controller 304, a network monitor 308, and a

US 6,832,249 B2

7

resource database 312. The network monitor 308 may be used to monitor a network element 314, which may be interconnected with other network elements (not shown) using communication links 318. Moreover, although only one network element 314 is shown, the network monitor 308 may be coupled to a multitude of network elements 314, which may be interconnected using any number of communication links 318. Generally, the network elements 314 function as nodes in a network, and the communication links 318 may be used to interconnect the nodes. For example, in one illustrative embodiment, an exemplary network element 314 may be located in AT&T's wide area network, and the communication links 318 may be used to interconnect the network element 314 with other network elements (not shown) in AT&T's wide area network. In another embodiment, the network element 314 may be located in a private network between two locations of a corporation (e.g., between Houston and Dallas), and the communication links 318 may represent the various circuits or communication routes that interconnect the network element 314 with other network elements (not shown) in the private network. In another example, the network element 314 may be a node in the Internet, and the communication links 318 may comprise the various communication paths that interconnect the network element 314 with other network elements (not shown) in the Internet.

Although the complexities of the network monitor 308 are not shown, those skilled in the art will appreciate that the network monitor 308 may be comprised of a variety of known devices. Moreover, the specific hardware and software implementation of the network monitor 308 may vary depending upon the particular implementation. However, in one illustrative embodiment, the network monitor 308 is a Sun Netra T1 server operating using the Solaris operating system.

The resource database 312 may be used to organize the functionality of the communication links 318 and the network elements 314 according to the OSI reference model. In one illustrative embodiment, the communication resources of the network element 314 may be comprised of IP routers, ATM switches, fiber lines, application services, and the like. Accordingly, the communication resources may be organized in the resource database 312 according to their functionality within the OSI reference model. For example, ATM switches may be categorized in the resource database 312 into layer 2, fiber lines may be categorized into layer 1, and application programs may be categorized in layer 7.

The control system 300 is capable of recognizing that communication resources (e.g., routers, fiber lines, etc.) may be shared or exclusive. Accordingly, the network monitor 308 correlates the information of the various communication links 318 and presents it to the resource database 312 in a logical manner. For example, the network monitor 308 may need to combine information from communication resources at multiple OSI layers or combine information from communication resources in the same OSI layer. Moreover, the network monitor 308 may also collect topological information related to the network element 314, and this information may also be included in the resource database 312. For example, the network monitor 308 may capture the site of location of a particular router, ATM switch, fiber line, etc. and the manner in which other devices are connected to it. To this end, the network monitor 308 may use standard industry techniques, such as simple network monitoring protocol (SNMP) and remote network monitoring (RMON) to perform its monitoring and reporting to the network controller 304 and the resource database 312.

8

The resource database 312 may comprise a dynamic listing of communication resources that are available in any network element 314. For example, the resource database 312 may be continually updated as new resources are added to the network element 314 and as old resources are removed. Moreover, the network monitor 308 and the network controller 304 may communicate with both the resource database 312 and the network element 314 to maintain an updated organized listing of the resources available in the network element 314. Those skilled in the art will appreciate that the resource database 312 may be stored on a separate storage device comprised of a variety of known storage devices, such as hard disk drives, and the like. Alternatively, in another embodiment, the resource database 312 may be incorporated with the network monitor 308 and/or the network controller 304.

The network controller 304 may communicate with the resource database 312, the network monitor 308, and the network element 314 using a signaling network 322. Those skilled in the art will appreciate that the signaling network 322 may be comprised of a variety of devices and operate using any number of known protocols. In one embodiment, the signaling network 322 is comprised of fiber lines, and the communication protocol is IP.

The network controller 304 and the network monitor 308 may communicate with the communication links 318, over the signaling network 322, by using existing communication ports and protocols of the communication resources (e.g., network devices, programs, protocols, etc.) functioning within the respective network elements 314. In one embodiment, InterAgent® communication messaging software is a portion of the implementation of the network controller 304 and the network monitor 308. The InterAgent® software is described in the U.S. Pat. No. 5,634,010, which is hereby incorporated by reference. Moreover, the network controller 304 and the network monitor 308 may have multiple device drivers each of which provides a different command language such as command line interface (CLI), to which Cisco System routers respond; command language used by AT&T for telco switches (TL1); common open policy service (COPS), which represent priority ranking commands; and system command languages.

Although the complexities of the network controller 304 are not shown, those skilled in the art will appreciate that the network controller 304 may be comprised of a variety of known devices. Moreover, the specific hardware and software implementation of the network controller 304 may vary depending upon the particular implementation. However, in one illustrative embodiment, the network controller 304 is a Sun Netra T1 server operating using a Solaris operating system.

Furthermore, although the network controller 304, the network monitor 308, and the resource database 312 are illustrated as separate devices, the functionality of each device may be implemented within a single device. Moreover, the specific embodiment of the control system 300 may vary depending upon the particular implementation.

Referring to FIG. 4, a method for providing broadband communications over a multi-layered network having a plurality of OSI reference model layers functioning therein is shown. This process is discussed with reference to FIG. 3 to simplify illustrating the present invention. It should be appreciated that the configuration of the control system 300, shown in FIG. 3, is just one of many possible solutions that may be used to implement the present invention. As a result,



US 6,832,249 B2

9

the particular details of the control system **300**, such as hardware, topography, connections, protocols, and the like, should be considered for the purpose of illustration and not for the purpose of limitation. As described above, the exact details of the control system **300** may vary depending upon the particular implementation. Furthermore, even though much of FIG. 4 will be discussed with reference to the Internet, it should be appreciated that the method depicted therein would be equally applicable to any communication system having a plurality of OSI reference model layers functioning therein.

At block **400**, the control system **300** monitors at least one OSI reference model layer operating in the network element **314**. As discussed above, the communication links **318** connected to each network element **314** may be categorized, in the resource database **312**, according to their functional layers of the OSI reference model. Accordingly, the network monitor **308** is capable of segmenting its monitoring of the communication links **318** based on its own categorization scheme, in the resource database **312**. For example, the network monitor **308** may focus its interest on the network layer (layer **3**) of the OSI reference model by monitoring routers and/or any other device associated with the IP protocol. Similarly, the network monitor **308** may focus its interest on the physical layer (layer **1**) of the OSI model by monitoring fiber lines, cable lines, and the like. Moreover, the network monitor **308** may focus its interest on the application layer (layer **7**) of the OSI model by monitoring application programs and the like.

The monitoring process of the network monitor **308** may be proactive, reactive, or both. In one illustrative embodiment, the network monitor **308** may monitor in a proactive manner by continually polling resources associated with the OSI layer being monitored. For example, at a predetermined time interval, the network monitor **308** may send an update request to the communication resources operating in the monitored layer of the network element **314**. In response, the communication resources may send the requested information back to the network monitor **308**.

In another embodiment, the network monitor **308** may monitor in a more reactive mode, wherein communication resources send alert signals to the network monitor **308** when predetermined alert thresholds are met. For example, an application program (e.g., a web browser), functioning at layer **7** of the OSI reference model, may alert the network monitor **308** when it is about to send time sensitive data through the network element **314**. As will be described below, once alerted, the network monitor **308** may signal the network controller **304** to take appropriate action in response to the alert from the application program.

As described above, some communication resources may be difficult to associate with a single OSI layer. Accordingly, the network monitor **308** may be required to monitor more than one OSI layer to capture an accurate state of the network element **314**. To accomplish this, the network controller **304** may access the resource database **312** to determine how to monitor the resources associated with a particular network element **314**. For example, regardless of how the network monitor **308** has categorized the communication resources in the resource database **312**, the network monitor **308** may re-access its classification scheme from the resource database **312**, and use it to facilitate monitoring the corresponding resources of a network element **314**. For example, in one illustrative embodiment, the network monitor **308** may continually loop through the entries in the resource database **312**, use the entries to associate communication resources with their corresponding communication

10

links **318**, and monitor the communication resources according to the classification schemes in the resource database **312**.

The network monitor **308** may monitor the communication resources of the various network elements **314** searching for quality of service events. Generally, a quality of service event may be defined as any event that effects the quality of service of data being sent across a communication system. Some exemplary quality of service measurements include error seconds, unavailable seconds, packet loss rate, transmission time (latency), jitter (deviations from an expected value), bandwidth throughput, and the like.

Depending upon the implementation, the network monitor **308** may define and monitor error seconds in a variety of ways. That is, the specific error second thresholds that the network monitor **308** searches for may vary depending upon the communication system. In one example, error seconds may take on its generally accepted meaning as applied to SONET circuits. However, in another illustrative embodiment, an error second may be defined as any second in which a minimum of one and a maximum of 44 bit errors have occurred. Similarly, severely errored seconds may be defined as any second in which there have been 45 or more bit errors. Finally, unavailable seconds may be a consecutive string of 10 or more severely errored seconds. For example, 9 consecutive severely errored seconds are not unavailable seconds, but 11 consecutive severely errored seconds are also 11 unavailable seconds.

Packet loss rate may be defined as the number of packets that are sent to a particular destination but do not arrive. Again, the network monitor **308** may define any arbitrary threshold value for packet loss rate, and the particular threshold value may vary depending upon the communication system. For example, if the network monitor **308** was ensuring a very high quality of service link between two points, the packet loss rate and the error second threshold values may be set low to ensure a high quality of service.

Transmission time (i.e., latency) may be defined as the time required to send data from a sending point to a destination point. As a practical matter, it is desirable to minimize transmission time. Jitter may be defined as deviations from the usual transmission time between the two points. For example, if a normal transmission requires 100 ms and, later, the same transmission takes 200 ms, then the jitter value for that particular communication link may be approximately 100 ms. Moreover, excessive transmission time and jitter may severely limit the ability to send rich media content across a communication link **318** (i.e., excessive transmission time and jitter may result in low quality of service) even when the communication link **318** has sufficient bandwidth for the transmission.

Bandwidth throughput is probably the most commonly used quality of service measurement. It is often defined as "the size of the pipe" between two points. For example, a DS-3 line may have a bandwidth throughput of 44.736 Mb/s, while an OC-1 line may have a bandwidth throughput of 51.84 Mb/s. Generally, a measurement of bandwidth throughput, alone, is insufficient to predict or gauge the quality of service that will be experienced between two points in a communication system. For example, even though a communication link may have a large bandwidth throughput, if the communication link produces a large value for error seconds, packet loss, or jitter, the quality of service experienced for the communication link may be very poor. As such, it may be necessary for the network monitor **308** to monitor a variety of quality of service measurements to ensure that a particular quality of service is maintained.

US 6,832,249 B2

11

Referring again to FIG. 4, at block 404, the network monitor 308 may determine that a quality of service event has occurred in the network element 314. As described above, the network monitor 308 may monitor various quality of service measurements in the network element 314. Determining whether a quality of service event has occurred may vary depending upon, for example, the quality of service measurement, the OSI reference model layer being monitored, the communication link 318, and the like. However, in one illustrative embodiment, the network monitor 308 may monitor a network element 314 for severely errored seconds, and if a severely errored seconds measurement is determined to occur in the network element 314, the network monitor 308 may determine that a quality of service event has occurred.

In another illustrative example, an application program (e.g., a web browser application) functioning at layer 7 of the OSI reference model may signal the network monitor 308 that it intends to send rich media content to a particular destination in the network element 314. This signal from the application program may be considered by the network monitor 308 to be a quality of service event.

It should be appreciated that a quality of service event may occur from any functional level of the OSI reference model. For example, the quality of service event may occur from an application program (layer 7), a router (layer 3), an ATM circuit (layer 2), an add drop multiplexer (ADM) of a fiber circuit (layer 1), etc. Moreover, the network monitor 308 may determine that a quality of service event has occurred in a network element 314 using proactive, reactive, or any other measuring technique.

In addition to the quality of service measurements, a quality of service event may be the addition or deletion of communication resources in a network element 314. For example, the network monitor 308 may be used to determine when additional communication resources (i.e., fiber lines, routers, ATM circuits, ATM switches, leased lines, new routing protocols, data delivery programs, hardware, software, etc.) have been added to a particular network element 314. When this occurs, the network monitor 308 may, among other things, determine that a quality of service event has occurred in the network element 314, update the resource database 312 with the new communication resources, and alert the network controller 304 respond.

Similarly, when communication resources are removed from a network element 314, either temporarily or permanently, the network monitor 308 may initiate a similar course of action. That is, the network monitor 308 may determine that a quality of service event has occurred in the network element 314, remove the resources from the resource database 312, and alert the network controller 304 to respond.

Once a quality of service event is detected, the network monitor 308 may determine that the quality of service event occurred at a layer N in the OSI reference model. For example, the network monitor 308 may use the resource database 312 to determine where in the OSI reference model the quality of service event occurred. In one illustrative embodiment, the network monitor 308 may determine that a particular router is experiencing a high packet loss rate (i.e., the network monitor 308 may determine that a quality of service event has occurred.) The network monitor 308 may then locate the router in the resource database 312 and determine that the quality of service event is occurring at the network layer of the OSI reference model (layer 3). Therefore, layer 3 would become layer N.

12

In another illustrative example, an application program may signal the network monitor 308 that it expects to send rich media content to a particular location in a network. Accordingly, the network monitor 308 may characterize the signal as a quality of service event. The network monitor 308 may then locate where in the OSI reference model the application program resides using the resource database 312. For example, the network monitor 308 may determine that the application program functions at layer 7 in the OSI reference mode. Therefore layer 7 would become layer N.

Referring back to FIG. 4, at block 408, the network controller 304 may respond to the quality of service event in the network element 314 by changing the network provisioning at a layer less than N. As described above, the resource database 312 organizes communication resources of the network element 314 according to where the communication resources fit in the OSI reference model. Additionally, the resource database 312 maintains the relationship between the various layers in the OSI model for the communication resources. For example, in one illustrative embodiment, a communication link 318, when viewed from the perspective of layer 3, may appear to be an IP path. Accordingly, the communication link 318 would be organized in the resource database 312 at layer 3. However, the IP path may also include a collection of fiber circuits that only appears to be an IP path when viewed from layer 3. Accordingly, in this illustrative example, the communication link 318 would also be organized in the resource database 312 under layer 1. The network monitor 308 and the resource database 312 maintain these relationships for all communication resources entered into the resource database 312.

In another illustrative embodiment, a communication link 318, may again appear to be solely an IP path when viewed from the perspective of layer 3. However, the IP path may also include a collection of fiber circuits, ATM circuits, leased lines, and the like. Accordingly, the communication link 318 would be organized in the resource database 312 under layer 3, layer 2, and layer 1. Again, the network monitor 308 and the resource database 312 maintain these relationships, which may be recalled upon request.

Referring back to FIG. 4, at block 412, when the network monitor 308 detects that a quality of service event has occurred in the network element 314, the network controller 304 may be called upon to respond to the quality of service event by changing the network provisioning at an OSI layer less than N. An illustrative example of this is shown in FIGS. 5A, 5B, and 5C.

Referring to FIG. 5A, a simplified illustrative communication system 500 is shown. It should be appreciated that much of the complexity of the communication system 500 has been removed for the purpose of simplifying the illustration of the present invention. When viewed from layer 3, the communication system 500 is comprised of a first user 504 coupled to a first router 508 over a first signaling line 512, and a second user 516 connected to a second router 520 over a second signaling line 524. A data line 528 is coupled between the first and second router 508, 520. In this embodiment, if the network monitor 308 determines that a quality of service event has occurred in the communication system 500, the network monitor 308, using the resource database 312, is likely to determine that the quality of service event has occurred at the network layer of the OSI reference model (layer 3). However, the network monitor 308 may use its knowledge of the communication system 500 and the resource database 312 to determine that the communication system 500 is actually made up of commu-

US 6,832,249 B2

13

nication resources occupying different levels of the OSI reference model.

Referring to FIG. 5B, when viewed from layer 2 and layer 1 of the OSI reference model, the communication system 500 may actually include additional communication resources, such as first and second add drop multiplexers 532, 536 and first and second STM-1 lines 540, 544 each having 155 Mb/s of bandwidth (310 Mb/s total.) Generally, the infrastructure of the communication system 500 residing in layer 2 and layer 1 of the OSI reference model is transparent when the communication system 500 is viewed from layer 3. That is, the first and second routers 508, 520 and the first and second users 504, 516, of FIG. 5A, may be unaware that the communication resources of FIG. 5B (e.g., ADM multiplexers, fiber lines, etc.) are used to transport data in the communication system 500. Moreover, if a quality of service event is occurring in the communication system 500, it may appear that the quality of service event is occurring at layer 3 (i.e., FIG. 5A), when the resolution to the quality of service event is really at layer 2 or layer 1 (i.e., FIG. 5B.)

Referring to FIG. 5C, once the network monitor 308 has determined that a quality of service event has occurred at layer 3 (FIG. 5A), the network monitor 308 may signal the network controller 304 to respond to the quality of service event in the communication system 500 by changing the network provisioning at an OSI layer less than N. In this illustrative example, the OSI layers less than N are layer 2 and layer 1. In FIG. 5C, the network monitor 308 has changed the network provisioning in the communication system 500 by activating third and fourth STM-1 lines 548, 552, thus, increasing the bandwidth between the first and second users 504, 516 to 620 Mb/s.

The decision to activate the third and fourth STM-1 lines 548, 552 may be based on a variety of factors, such as the type of quality of service event, past history with the third and fourth STM-1 lines 548, 552, the characteristics of the data being sent between the first and second users 504, 516 (e.g., media rich content), and the like. For example, if the quality of service event was based on error seconds, the third and fourth STM-1 lines 548, 552 may have been activated because they were known to produce relatively few error seconds. Alternatively, the network controller 304 may base the decision on availability, that is, the network controller 304 may use the additional capacity as a hedge against future error seconds (i.e., error seconds and bandwidth may be inversely related.)

In another illustrative embodiment, the quality of service event may be a signal from an application of the first user 504 that the application is about to send a large amount of data to the second user 516. In this example, the quality of service event may appear to the network controller 304 to be occurring at the application layer of the OSI reference model. Accordingly, layer N, in the OSI reference model, would become layer 7, and the layers less than N may be OSI layers 6 through 1. Using the resource database 312, the network monitor 308 may signal the network controller 304 to respond to the quality of service event by changing the network provisioning in the communication system 500 at an OSI layer less than N. As a result, the network controller 304 may take similar action, as described above, and activate the third and fourth STM-1 lines 548, 552, illustrated in FIG. 5C.

Alternatively, rather than activating the third and fourth STM-1 lines 548, 552, the network controller 304 may change the network provisioning by balancing the transmis-

14

sion load carried between the first and second STM-1 lines 540, 544. For example, if the first user 504 is about to send a large amount of data to the second user 516, in response to this quality of service event (i.e., a layer 7 event), the network controller 304 may adjust the load on the first and second STM-1 lines 540, 544, such that the connection between the first and second users 504, 516 is allotted additional bandwidth.

Once the transmission is complete, the application operating at the first user 504 may send an additional quality of service signal to the network monitor 308 that the transmission is complete. The network monitor 308 may then signal the network controller 304 to respond to the quality of service event, and the network controller 304 may readjust the load on the first and second STM-1 lines 540, 544 back to its previous state.

In yet another illustrative embodiment, referring back to FIG. 5A, the network monitor 308 may determine that a quality of service event has occurred in the communication system 500. As described above, the network monitor 308 is likely to determine that the quality of service event has occurred at the network layer of the OSI reference model (layer 3), and the resolution to the quality of service event is likely to be at an OSI layer less than 3. When this occurs, rather than or in addition to provisioning additional circuits between the first and second routers 508, 520, the network controller 304 may respond to the quality of service event using multiprotocol label switching (MPLS).

Generally, MPLS involves setting up a specific path for a given sequence of packets, which may be identified by a label inserted in each packet. In this example, rather than looking up the address to the next network element 314, the first or second routers 508, 520 may be able to forward the packet to its next destination based on its label. In other words, MPLS typically allows for packets to be forwarded at the layer 2 (switching) level rather than at layer 3. Thus, a quality of service event in layer 3 may be resolved by changing the network provisioning at layer 2, using MPLS.

The network controller 304 may use MPLS to respond to a layer 3 or any other OSI layer quality of service event by controlling and determining the particular route data packets traverse through a network. For example, if a quality of service event is occurring at a particular network element 314, the network controller 304 may use MPLS to route data traffic away from the problem causing network element 314. Additionally, the network controller 304 may use MPLS to balance or distribute the traffic load across the network. Furthermore, the network controller 304 may resolve a quality of service event using MPLS by ensuring that the offending data packet traverse the shortest path possible to reach their destination. Generally, there are a variety of schemes the network controller 304 may apply using MPLS to resolve a quality of service event occurring at an OSI layer greater than 2 (i.e., layers 3-7).

Referring back to FIG. 4, as described above for block 412, the network controller may respond to the quality of service event in a multi-layered network by changing the network provisioning at a layer less than N. Although this may be accomplished by provisioning an additional circuit or path, as shown in FIGS. 5B and 5C, a change in the network provisioning may occur without the addition of any new communication circuits or paths. For example, the network controller may respond to a quality of service event by changing the path of an MPLS tunnel or by changing the priority on a queue in an IP router. Accordingly, for the purpose of the present invention, any change in the



US 6,832,249 B2

15

configuration, operation, characteristics, properties, etc. of communication resources in a network may be described as a change in network provisioning.

At block 416, if the network provisioning has been changed at the OSI layer less than N, the network controller 304 may signal the network monitor 308 that the change in the network provisioning is complete. The network monitor 308 may then update the resource database 312 with the change in network provisioning, and the network monitor 308 may continue to monitor the network element 314, waiting for quality of service events to occur.

Referring to FIGS. 6A through 6D, another illustrative example is shown. In FIG. 6A, a communication system 600 is shown connecting first and second users 604, 608. As described above, from the perspective of layer 7 and layer 3 of the OSI reference model, the communication system 600, more specifically the connection between the first and second users 604, 608, appears to be a plurality of routers 612 coupled together by a data line 616. However, referring to FIG. 6B, if the communication system 600 is viewed from layer 7, layer 3, and layer 2, of the OSI reference model, additional communication resources appear.

In FIG. 6B, the communication system 600 may appear, in this illustrative embodiment, as an IP cloud 620 having an ATM cloud 624 functioning therein. For example, the first user 604 may be coupled to the IP cloud 620 through a first access router 628, and the first access router 628 may be coupled to the ATM cloud 624 using a first concentrator router 632. Similarly, the second user 608 may be coupled to the IP cloud 620 through a second access router 636, and the second access router 636 may be coupled to the ATM cloud 624 using a second concentrator router 640. Again, many of the complexities of the communication system 600 have been removed to simplify illustrating the present invention.

Referring to FIG. 6C, an illustrative example of the ATM cloud 624 is shown. In this example, the ATM cloud 624 is comprised of multiplexers 644 and first and second virtual circuits 648, 652. Moreover, the virtual circuits 648, 652 may be permanent virtual circuits or switched virtual circuits. As described above, if the network monitor 308 determines that a quality of service event has occurred at a layer N, the network controller 304 may respond to the quality of service event by changing the network provisioning at an OSI layer less than N.

Referring to FIG. 6D, if the network monitor 308 determines that a quality of service event has occurred at OSI layer 3 (FIG. 6A), the network controller 304 may respond to the quality of service event by changing the network provisioning at layer 2 or layer 1 of the OSI model. For example, in FIG. 6D, the network controller 304 has provisioned a third virtual circuit 656 in response to the quality of service event.

In another embodiment, the quality of service event, at layer 3, may be the activation of the third virtual circuit 656. For example, as networks grow, additional communication resources are continually being brought online. When this occurs, the newly added resources (e.g., the third virtual circuit 656) may appear at layer 3 (FIG. 6A) as an increase in available throughput capacity, thus, triggering a quality of service event at layer 3. In response to the quality of service event, the network controller 304 may provision the newly added third virtual circuit 656 for communication between the first and second user 632, 636. As described above, once the change in network provisioning is complete, the network controller 304 may send a signal to the network monitor 308, and the network monitor 308 may update the resource database 312.

16

As indicated above, aspects of this invention pertain to specific "method functions" implementable through various computer systems. In an alternate embodiment, the invention may be implemented as a computer program product for use with a computer system. Those skilled in the art should readily appreciate that programs defining the functions of the present invention can be delivered to a computer in many forms, which include, but are not limited to: (a) information permanently stored on non-writeable storage media (e.g., read only memory devices within a computer such as ROMs or CD-ROM disks readable only by a computer I/O attachment); (b) information alterably stored on writeable storage media (e.g., floppy disks and hard drives); or (c) information conveyed to a computer through communication media, such as a local area network, a telephone network, or a public network like the Internet. It should be understood, therefore, that such media, when carrying computer readable instructions that direct the method functions of the present invention, represent alternate embodiments of the present invention.

The particular embodiments disclosed above are illustrative only, as the invention may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. Furthermore, no limitations are intended to the details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope and spirit of the invention. Accordingly, the protection sought herein is as set forth in the claims below.

What is claimed:

1. A method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein, comprising:

- monitoring at least one OSI reference model layer functioning in the multi-layered network;
- determining that a quality of service event has occurred in the multi-layered network;
- determining that the quality of service event occurred at layer 3 in the OSI reference model and that the layer 3 quality of service event is related to an Internet Protocol (IP);
- responding to the quality of service event in the multi-layered network by changing network provisioning at layer 1 in the OSI reference model, wherein the change at layer 1 includes provisioning additional fiber optic circuits in the multi-layered network; and
- signaling that the network provisioning at layer 1 of the OSI reference model has been changed.

2. The method of claim 1 further comprising:

- segmenting the multi-layered network into communication resources; and
- organizing the communication resources into a classification scheme based on the functionality of the communication resources and the OSI reference model, wherein the classification scheme maintains the relationships between the communication resources and the OSI reference model.

3. The method of claim 2, wherein the classification scheme is stored in a resource database and monitoring at least one OSI reference model layer functioning in the multi-layered network comprises:

- looping through the resource database to re-access the classification scheme; and

US 6,832,249 B2

17

monitoring the communication links according to the classification scheme in the resource database.

4. The method of claim 3, wherein signaling that the network provisioning in the layer less than N has been changed comprises updating the resources database with the change in the network provisioning.

5. The method of claim 1, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network has insufficient bandwidth.

6. A method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein, comprising:

monitoring at least one OSI reference model layer functioning in the multi-layered network;

determining that a quality of service event has occurred in the multi-layered network;

determining that the quality of service event occurred at layer 3 in the OSI reference model and that the layer 3 quality of service event is related to an Internet Protocol (IP);

responding to the quality of service event in the multi-layered network by changing network provisioning at layer 2 in the OSI reference model, wherein the change at layer 2 includes provisioning additional ATM virtual circuits; and

signaling that the network provisioning at layer 2 of the OSI reference model has been changed.

7. The method of claim 6 further comprising:

segmenting the multi-layered network into communication resources; and

organizing the communication resources into a classification scheme based on the functionality of the communication resources and the OSI reference model, wherein the classification scheme maintains the relationships between the communication resources and the OSI reference model.

8. The method of claim 7, wherein the classification scheme is stored in a resource database and monitoring at least one OSI reference model layer functioning in the multi-layered network comprises:

looping through the resource database to re-access the classification scheme; and

monitoring the communication links according to the classification scheme in the resource database.

9. The method of claim 8, wherein signaling that the network provisioning in the layer less than N has been changed comprises updating the resources database with the change in the network provisioning.

10. The method of claim 6, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network has insufficient bandwidth.

11. A method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein, comprising:

monitoring at least one OSI reference model layer functioning in the multi-layered network;

determining that a quality of service event has occurred in the multi-layered network;

determining that the quality of service event occurred at a layer N in the OSI reference model;

responding to the quality of service event in the multi-layered network by changing network provisioning at a layer less than N; and

18

signaling that the network provisioning at the layer less than N has been changed.

12. The method of claim 11 further comprising:

segmenting the multi-layered network into communication resources; and

organizing the communication resources into a classification scheme based on the functionality of the communication resources and the OSI reference model, wherein the classification scheme maintains the relationships between the communication resources and the OSI reference model.

13. The method of claim 12, wherein the classification scheme is stored in a resource database and monitoring at least one OSI reference model layer functioning in the multi-layered network comprises:

looping through the resource database to re-access the classification scheme; and

monitoring the communication links according to the classification scheme in the resource database.

14. The method of claim 13, wherein signaling that the network provisioning in the layer less than N has been changed comprises updating the resources database with the change in the network provisioning.

15. The method of claim 11, wherein the quality of service event in the multi-layered network occurs at layer 3 in the OSI reference model and responding to the quality of service event comprises provisioning additional OSI layer 2 circuits in a communication link of the multi-layer network.

16. The method of claim 15, wherein the quality of service event at layer 3 in the OSI reference model is related to an internet protocol (IP) and responding to the quality of service event comprises provisioning additional ATM virtual circuits.

17. The method of claim 15, wherein the quality of service event at layer 3 in the OSI reference model is related to an internet protocol (IP) and responding to the quality of service event through OSI layer 2 comprises resolving the quality of service event using multiprotocol label switching (MPLS).

18. The method of claim 11, wherein determining that a quality of service event has occurred at a layer N in the multi-layered network comprises determining that additional communication resources have been brought online in the multi-layered network.

19. The method of claim 18, wherein responding to the quality of service event in the multi-layered network comprises provisioning the additional communication resources to a network element in the multi-layer network, wherein the network element has an OSI layer less than N functioning therein.

20. The method of claim 11, wherein the quality of service event in the multi-layered network occurs at layer 3 in the OSI reference model and responding to the quality of service event comprises provisioning additional OSI layer 1 circuits in a communication link of the multi-layer network.

21. The method of claim 20, wherein the quality of service event at layer 3 in the OSI reference model is related to an internet protocol (IP) and provisioning additional OSI layer 1 circuits comprises provisioning additional fiber optic circuits.

22. The method of claim 11, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network has insufficient bandwidth.

23. The method of claim 11, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network is exhibiting excessive latency.

US 6,832,249 B2

19

24. The method of claim 11, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network is exhibiting excessive packet loss.

25. The method of claim 11, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network is exhibiting excessive jitter.

26. The method of claim 11, wherein determining that a quality of service event has occurred at a layer N in the multi-layered network comprises determining that a group of communication resources are no longer operating in the multi-layered network.

27. The method of claim 11, wherein the quality of service event in the multi-layered network occurs at layer 3 in the OSI reference model and responding to the quality of service event comprises balancing bandwidth demand in existing layer 1 circuits of the multi-layered network.

28. The method of claim 11, wherein the quality of service event in the multi-layered network occurs at layer 7 in the OSI reference model and responding to the quality of service event comprises provisioning additional OSI layer 1 circuits in a communication link of the multi-layer network.

29. The method of claim 11 wherein monitoring at least one OSI reference model layer functioning in the multi-layered network comprises monitoring communication resources of the multi-layered network using a proactive monitoring process.

30. The method of claim 11 wherein monitoring at least one OSI reference model layer functioning in the multi-layered network comprises monitoring communication resources of the multi-layered network using a reactive monitoring process.

31. A method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein, comprising:

monitoring at least one OSI reference model layer functioning in the multi-layered network;

determining that a quality of service event has occurred in the multi-layered network;

determining that the quality of service event occurred at layer 3 in the OSI reference model and that the layer 3 quality of service event is related to an Internet Protocol (IP);

responding to the quality of service event in the multi-layered network by changing network provisioning at layer 2 in the OSI reference model, wherein the change at layer 2 includes resolving the quality of service event using multiprotocol label switching (MPLS); and

signaling that the network provisioning at layer 2 of the OSI reference model has been changed.

32. The method of claim 31 wherein resolving the quality of service event using multiprotocol label switching further comprises balancing data traffic throughout the network.

33. The method of claim 32, wherein balancing the data traffic throughout the network comprises routing time sensitive data through the shortest possible path in the network.

34. The method of claim 31 further comprising:

segmenting the multi-layered network into communication resources; and

organizing the communication resources into a classification scheme based on the functionality of the communication resources and the OSI reference model, wherein the classification scheme maintains the rela-

20

tionships between the communication resources and the OSI reference model.

35. The method of claim 34, wherein the classification scheme is stored in a resource database and monitoring at least one OSI reference model layer functioning in the multi-layered network comprises:

looping through the resource database to re-access the classification scheme; and

monitoring the communication links according to the classification scheme in the resource database.

36. The method of claim 31 wherein resolving the quality of service event using multiprotocol label switching further comprises:

determining a location of the quality of service event in the multi-layered network; and

using MPLS to route data traffic away from the quality of service event.

37. The method of claim 31, wherein determining that a quality of service event has occurred in the multi-layered network comprises determining that a communication link in the multi-layered network has insufficient bandwidth.

38. A system for providing broadband communications, comprising:

a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein;

a network monitor coupled to the multi-layered network, wherein the network monitor is adapted to:

monitor at least one OSI reference model layer functioning in the multi-layered network;

determine that a quality of service event has occurred in the multi-layered network; and

determine that the quality of service event occurred at layer N in the OSI reference model; and

a network controller coupled to the multi-layered network and the network monitor, wherein the network controller is adapted to:

respond to the quality of service event in the multi-layered network by changing the network provisioning at a layer less than N.

39. The system of claim 38, further comprising:

a resource database coupled to the network monitor, wherein the network monitor organizes communication resources of the multi-layer network into a classification scheme based on the functionality of the communication resources and the OSI reference model, and the classification scheme maintains the relationship between the communication resources and the OSI reference model, which is stored in the resource database.

40. The system of claim 39, further comprising additional communication resources in the multi-layered network wherein the network monitor signals the resource data base that additional communication resources have been brought on line, and the additional communication resources are stored in the resource database.

41. The system of claim 38, wherein the multi-layered network comprises an OSI layer 2 circuit that was provisioned by the network controller in response to a quality of service event at OSI layer 3 in the multi-layered network.

42. The system of claim 38, wherein the multi-layered network comprises an OSI layer 1 circuit that was provisioned by the network controller in response to a quality of service event at OSI layer 3 in the multi-layered network.

43. The system of claim 38, wherein the multi-layered network comprises an OSI layer 2 circuit that was provi-

US 6,832,249 B2

21

sioned by the network controller in response to a quality of service event at OSI layer 7 in the multi-layered network.

44. The system of claim 38, wherein the multi-layered network comprises an OSI layer 1 circuit that was provisioned by the network controller in response to a quality of service event at OSI layer 7 in the multi-layered network.

45. The system of claim 38, wherein the multi-layered network comprises layer 3 network elements that were configured by the network controller in response to a quality of service event at OSI layer 7 in the multi-layered network.

46. The system of claim 38, wherein the network monitor monitors communication resources of the multi-layered network using a proactive monitoring process.

47. The system of claim 38, wherein the network monitor monitors communication resources of the multi-layered network using a reactive monitoring process.

48. A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method for providing broadband communications over a multi-layered network having a plurality of Open System Interconnection (OSI) Reference Model layers functioning therein, comprising:

- monitoring at least one OSI reference model layer functioning in the multi-layered network;
- determining that a quality of service event has occurred in the multi-layered network;

22

determining that the quality of service event occurred at a layer N in the OSI reference model;

responding to the quality of service event in the multi-layered network by changing network provisioning at a layer less than N; and

signaling that the network provisioning at the layer less than N has been changed.

49. A system for providing broadband communications, comprising:

- means for monitoring at least one OSI reference model layer functioning in the multi-layered network;
- means for determining that a quality of service event has occurred in the multi-layered network;
- means for determining that the quality of service event occurred at a layer N in the OSI Reference Model;
- means for responding to the quality of service event in the multi-layered network by changing network provisioning at a layer less than N; and
- means for signaling that the network provisioning at the layer less than N has been changed.

\* \* \* \* \*

# Exhibit F

---





US006891807B2

(12) **United States Patent**  
**Roskind et al.**

(10) **Patent No.:** **US 6,891,807 B2**  
(45) **Date of Patent:** **May 10, 2005**

(54) **TIME BASED WIRELESS ACCESS  
PROVISIONING**

(75) Inventors: **James A. Roskind**, Redwood City, CA  
(US); **John D. Robinson**, South Riding,  
VA (US)

(73) Assignee: **America Online, Incorporated**, Dulles,  
VA (US)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 94 days.

(21) Appl. No.: **10/341,847**

(22) Filed: **Jan. 13, 2003**

(65) **Prior Publication Data**

US 2004/0165546 A1 Aug. 26, 2004

(51) **Int. Cl.**<sup>7</sup> ..... **H04L 12/26; H04Q 7/34**

(52) **U.S. Cl.** ..... **370/255; 370/338**

(58) **Field of Search** ..... 370/254, 255,  
370/338; 455/422, 435, 410, 411; 380/247

(56) **References Cited**

#### U.S. PATENT DOCUMENTS

5,461,627	A *	10/1995	Rypinski	370/346
6,058,106	A	5/2000	Cudak et al.	370/313
6,167,428	A	12/2000	Ellis	709/201
6,272,129	B1	8/2001	Dynarski et al.	370/356
6,275,693	B1	8/2001	Lin et al.	455/414
6,282,183	B1	8/2001	Harris et al.	370/338
6,317,594	B1	11/2001	Gossman et al.	455/414
6,334,056	B1	12/2001	Holmes et al.	455/445
6,359,880	B1	3/2002	Curry et al.	370/352
6,418,146	B1	7/2002	Miloslavsky	370/400
6,418,324	B1	7/2002	Doviak et al.	455/556
2001/0048744	A1 *	12/2001	Kimura	380/247
2003/0152235	A1 *	8/2003	Cohen et al.	380/278

#### FOREIGN PATENT DOCUMENTS

EP 814 623 12/1997 ..... H04Q/7/22

EP	999 672	5/2000	.....	H04L/12/28
EP	1 081 895	3/2001	.....	H04L/12/28
EP	1 126 681	8/2001	.....	H04L/29/06
EP	1 191 763	3/2002	.....	H04L/29/06
EP	1 225 778	7/2002	.....	H04Q/7/38
JP	2001-308866	11/2001	.....	H04L/12/28
WO	WO 01/22661	3/2001	.....	H04L/12/28

#### OTHER PUBLICATIONS

*Microsoft Announces Wireless Provisioning Services*; Geek-  
Zone; Wi-Fi, posted Dec. 10, 2003 20:56:21 NZ.

*HP Spotlights Mobile Gear*; Ina Fried; CNET News.com;  
Oct. 13, 2003.

*Wireless Provisioning Services Overview*; The Cable Guy—  
Dec. 2003; TechNet Newsletter; 2004 Microsoft Corpora-  
tion.

(Continued)

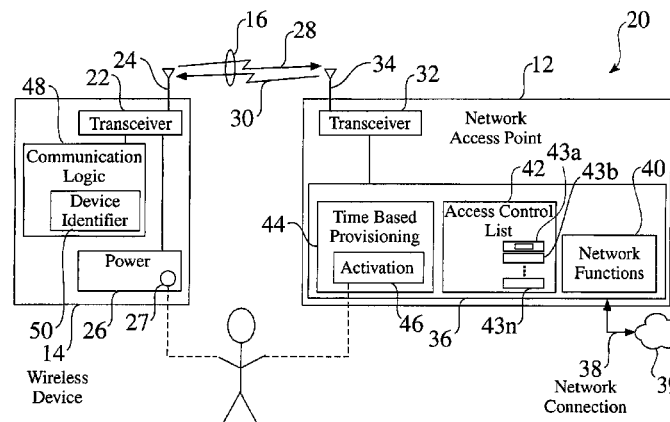
*Primary Examiner*—Melvin Marcelo

(74) *Attorney, Agent, or Firm*—Glenn Patent Group;  
Michael A. Glenn

(57) **ABSTRACT**

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter (such as power on or the onset of signal transmission) of the wireless device occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. In one system embodiment, the network access point tracks the power on time of wireless devices. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

**71 Claims, 7 Drawing Sheets**





**US 6,891,807 B2**

Page 2

**OTHER PUBLICATIONS**

Sony Ericsson Mobile Communications; *Sony Ericsson HBH-65* (Manual); Pub #LZT 1086746 R1A; 1<sup>st</sup> Ed. Aug. 2003; Sony Ericsson Mobile Communications, AB.

*Security Issues for Wearable Computing and Bluetooth Technology*; Catharina Candolin, undated.

*Privacy and Authentication for Wireless Local Area Networks*; Ashar Aziz, and Whitfield Diffie; Sun Microsystems, Inc.; Jul. 26, 1993.

*Painting Your Home Blue [Bluetooth/sup TM/wireless Technology]*; D. Cypher; Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances; Jan. 15–16, 2002.

*Wireless Home Networks Based on a Hierarchical Bluetooth Scatternet Architecture*; W. Lilakiatsakun, A. Seneviratne; Proceedings Ninth IEEE International Conference on Networks; Oct. 10–12, 2001.

*Bluetooth Wireless Technology in the Home*; R. Sheperd; Electronics & Communication Engineering Journal; Oct. 2001.

*Wireless Gateway for Wireless Home AV Network and Its Implementation*; T. Saito, I. Imoda, Y. Takabatke, and K. Teramoto, and K. Fujimoto; IEEE Transactions on consumer Electronics; Aug. 2001.

*A Wireless Home Network and Its Application Systems*; H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura; IEEE Transactions on Consumer Electronics; May 2000.

*Wireless Home Link*; M. Nakagawa; IEICE Transactions on Communications; Dec. 1999.

*An Access Protocol for a Wireless Home Network*; A.C.V. Gummalla, and J.O. Limb; WCNC. 1999 IEEE Wireless Communications and Networking Conference; Sep. 21–24, 1999.

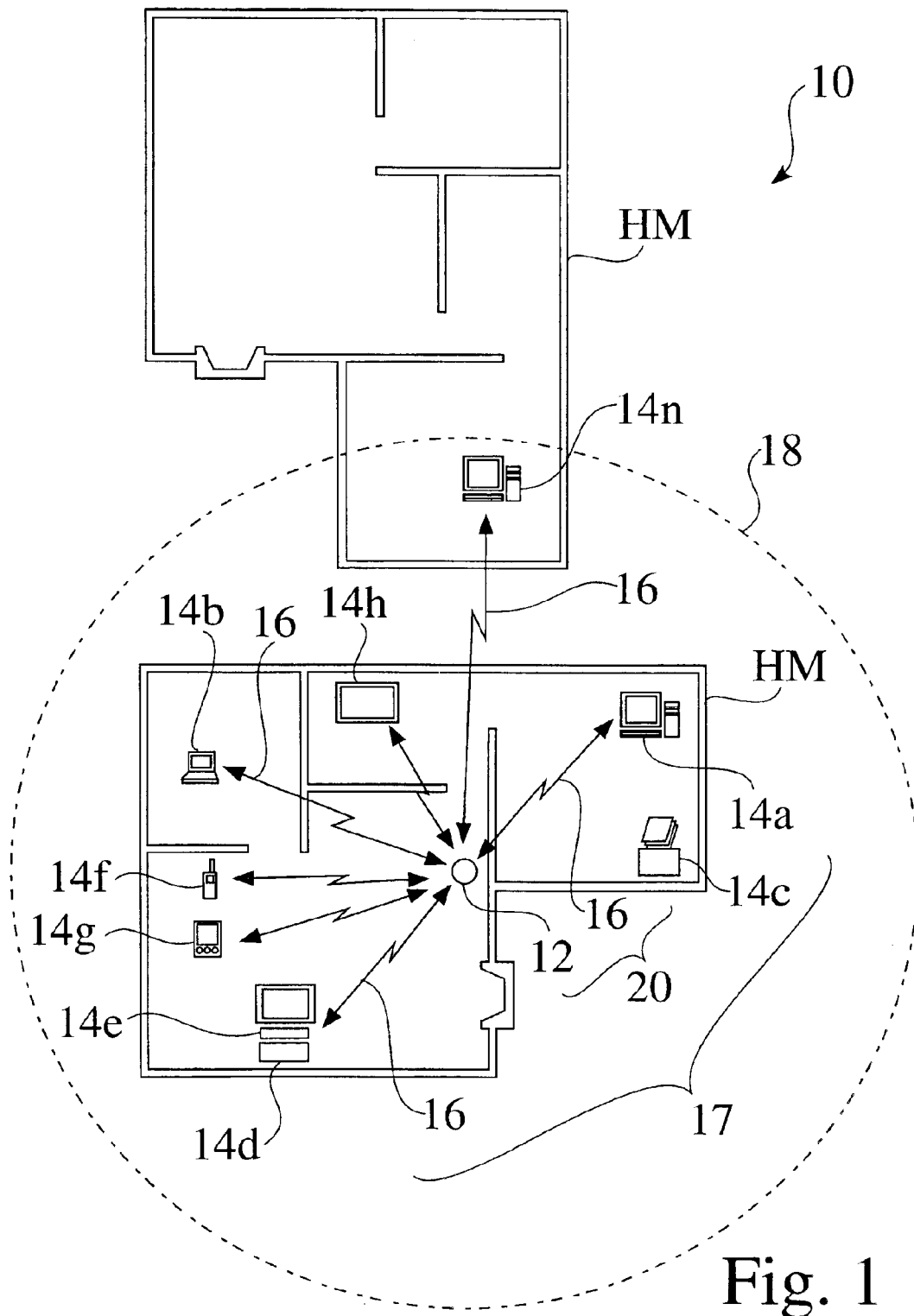
*Firewalls for Security in Wireless Networks*; U. Murthy, O. Bukhres, W. Winn, and E. Vanderdez; Proceedings of the Thirty-First Hawaii International Conference on System sciences; Jan. 6–9, 1998.

*Self-Securing Ad Hoc Wireless Networks*; Haiyun Luo, Petros Aerfos, Jiejun Kng, Songwu Lu, and Lixia Zhang, undated.

*Wireless Networking for Control and Automation of Off-Road Equipment*; by J.D. Will; An ASAE Meeting Presentation, undated.

*Intrusion Detection in Wireless Ad-Hoc Networks*; Yongguang Zhang and Wenke Lee; Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking; Aug. 6–11, 2000.

\* cited by examiner



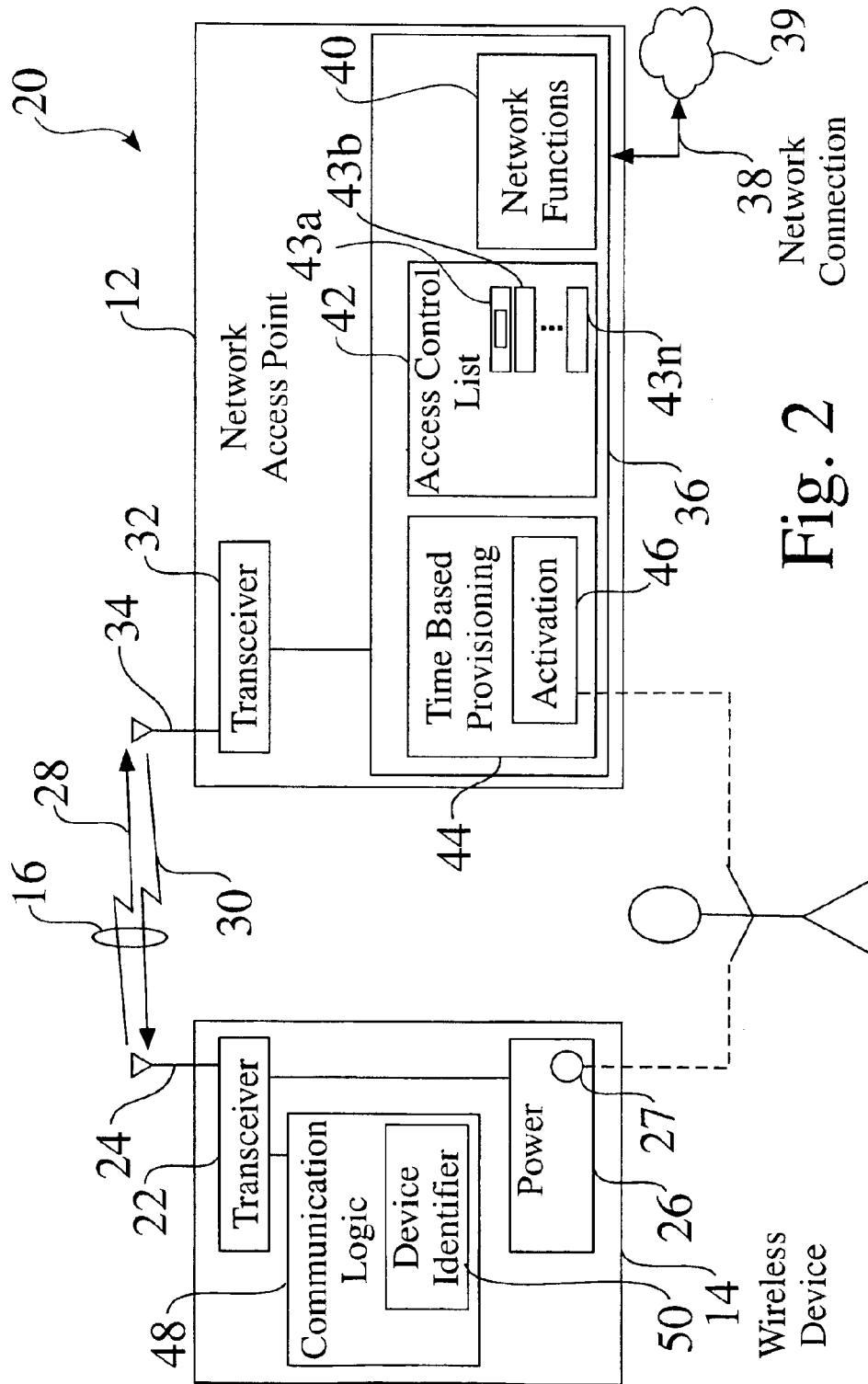


Fig. 2

U.S. Patent

May 10, 2005

Sheet 3 of 7

US 6,891,807 B2

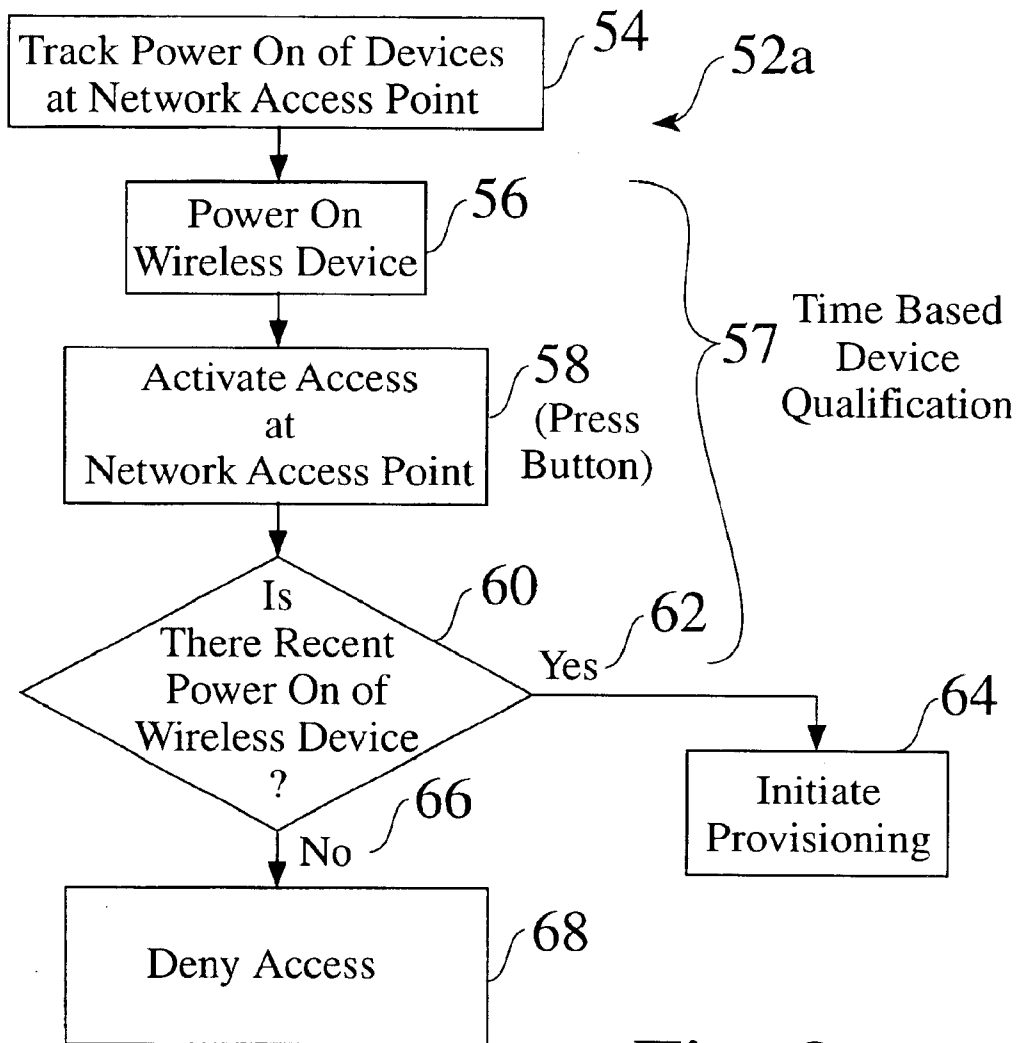


Fig. 3

U.S. Patent

May 10, 2005

Sheet 4 of 7

US 6,891,807 B2

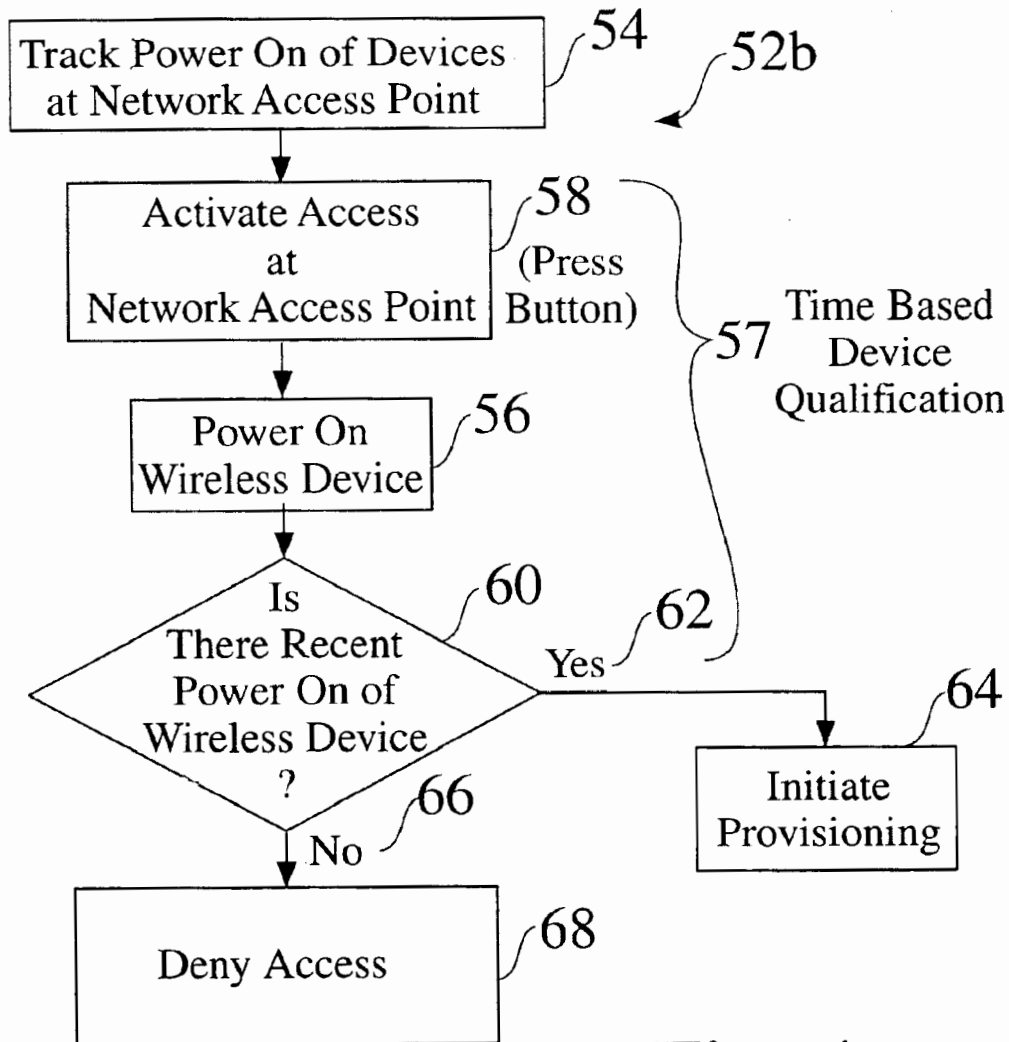


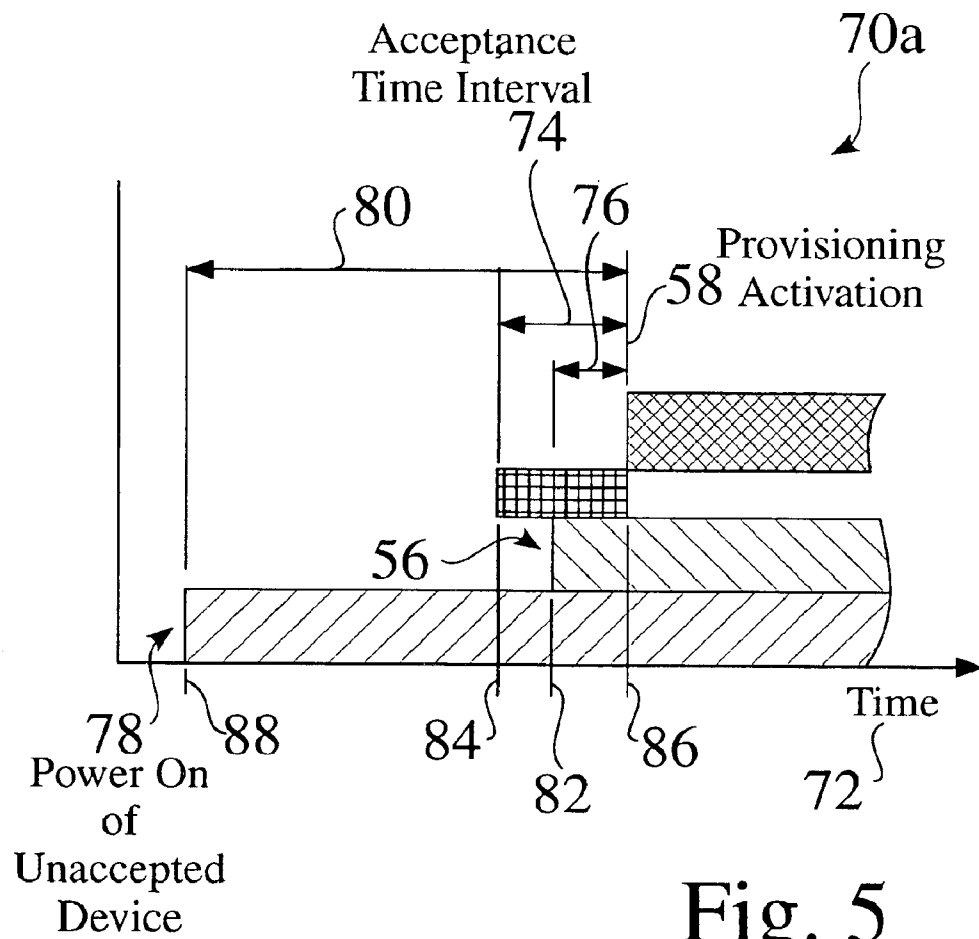
Fig. 4

**U.S. Patent**

May 10, 2005

Sheet 5 of 7

**US 6,891,807 B2**



**Fig. 5**



U.S. Patent

May 10, 2005

Sheet 6 of 7

US 6,891,807 B2

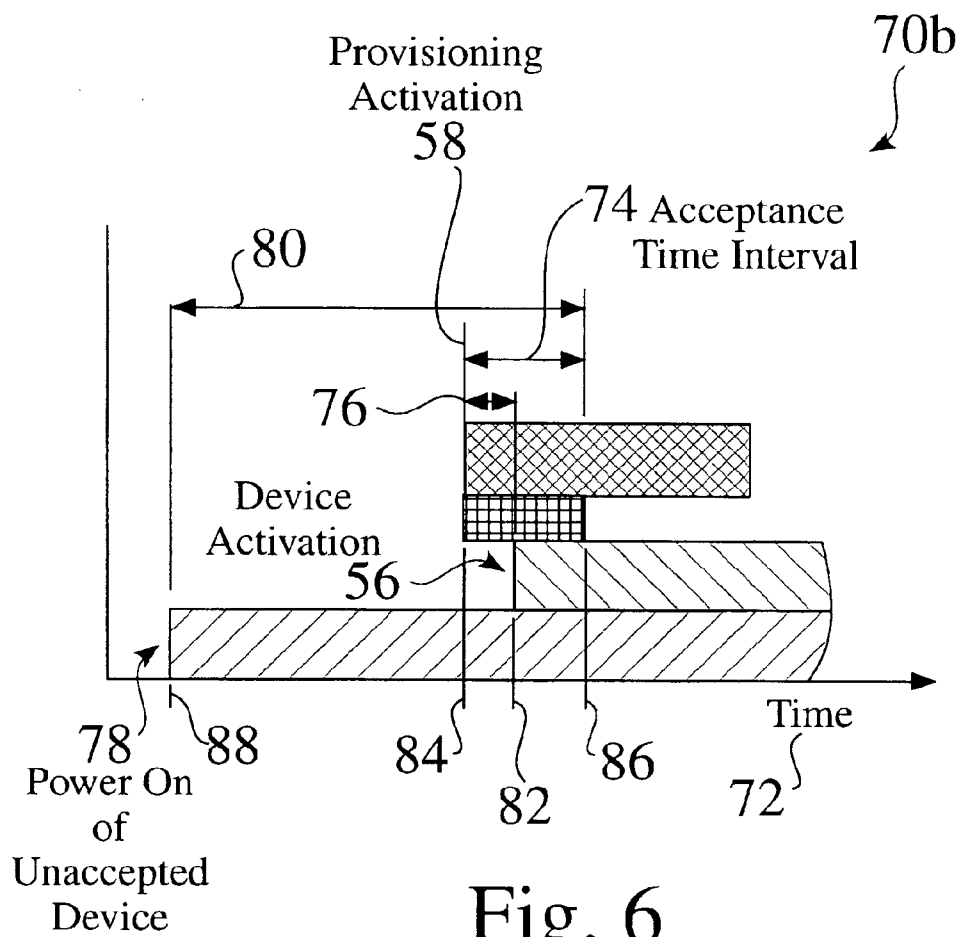


Fig. 6

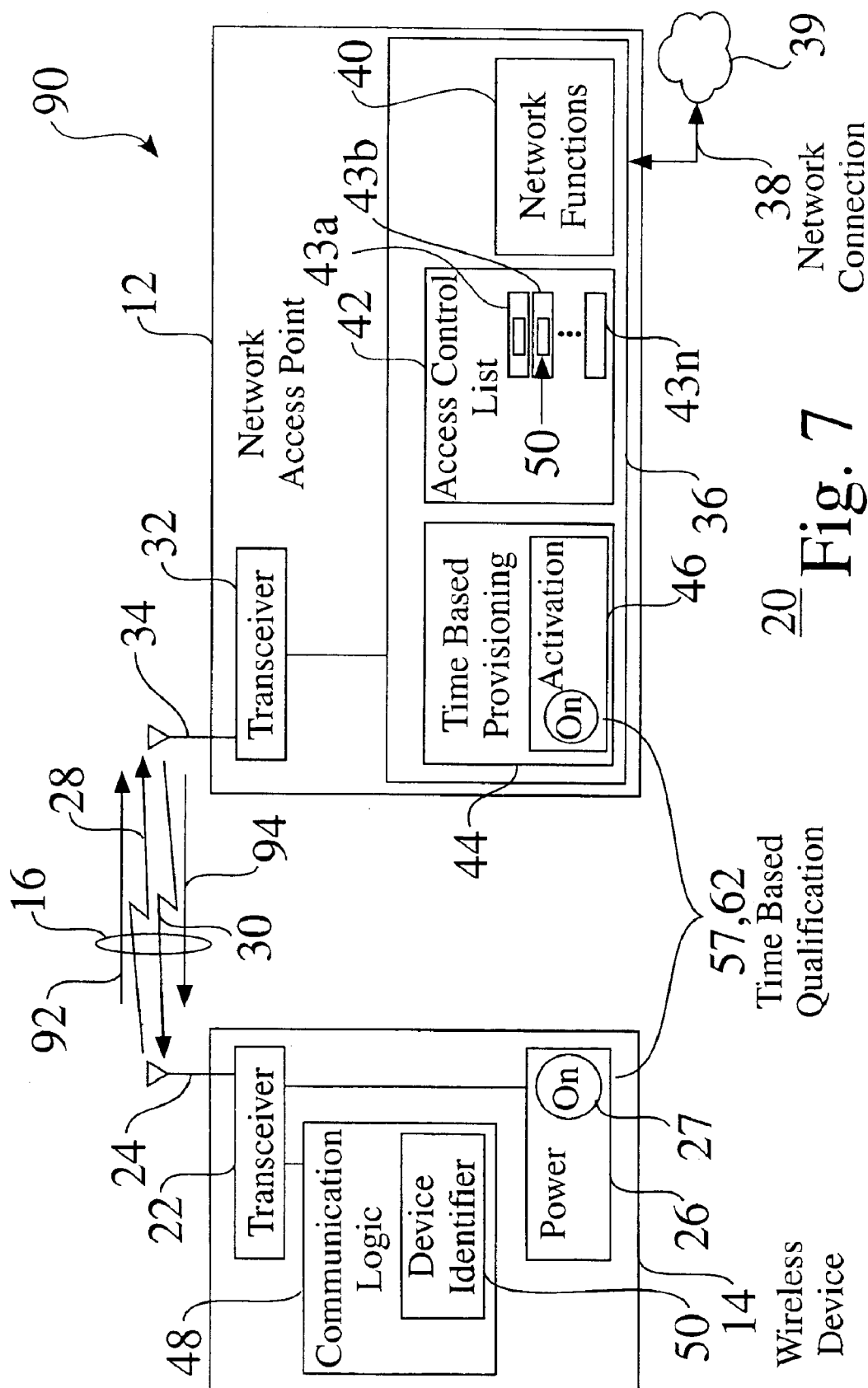


Fig. 7

US 6,891,807 B2

1

## TIME BASED WIRELESS ACCESS PROVISIONING

### FIELD OF THE INVENTION

The invention relates to the field of wireless connections between a wireless device and a network. More particularly, the invention relates to access provisioning between one or more wireless devices and an intranet access point.

### BACKGROUND OF THE INVENTION

In local area networks, such as wireless home networks, one or more wireless devices, e.g. such as IEEE 802.11b devices, are linked to the network by a provisioning process through a network access point. When a user acquires a new wireless device, they need to securely tie it to their intranet, which comprises telling the intranet to accept wireless communications from the device, as well as provisioning the device with key material, such as for creating an encrypted connection. In conventional networks having one or more devices to be provisioned to a network access point, device identification information, such as a MAC address, is required to be communicated from the wireless device to the access point.

Several methods have been described for wireless access provisioning to integrate wireless devices into a network.

M. Cudak, B. Mueller, J. Kelton, and B. Classon, Network Protocol Method, Access Point Device and Peripheral Devices for Providing for an Efficient Centrally Coordinated Peer-to-Peer Wireless Communications Network, U.S. Pat. No. 6,058,106, disclose a "peer-to-peer wireless communications network wherein the access point device: (1) broadcasts a block assignment that specifies a wireless source peripheral device and a wireless destination peripheral device; (2) receives, from the wireless destination peripheral device, sequence information; (3) determines whether the sequence information represents one of: a negative acknowledgment and a positive acknowledgment with a sequence number; (4) forwards an acknowledgment to the wireless source peripheral based on the sequence information, and repeats steps (1)–(4) until N blocks of data, N a predetermined integer, have been transferred from the wireless source peripheral to the wireless destination peripheral."

J. Lin, P. Alfano, and S. Upp, Method and Apparatus for Performing Bearer Independent Wireless Application Service Provisioning, U.S. Pat. No. 6,275,693 disclose a provisioning system, in which a "mobile communication device contacts a provisioning proxy over the wireless bearer network, which in turns contacts a provisioning center over a public network. A provisioning tunnel is then established between the provisioning center and the mobile communication device. Once the provisioning tunnel is set up, the user of the mobile communication device can subscribe to, or unsubscribe from wireless application services."

Wireless Device Registering Method in Wireless Home Network, PCT Patent Application Ser. No. WO 01/2266, describes the sending of an authentication key to a device for storage, when an identification code received from the device corresponds to a code stored in an access point.

Secure Wireless LAN, European Pat. No. EP, 1081895, discloses wireless device use by a wireless device operator with an access point connected to a wired LAN in communication with the wireless device through air channel authentication.

C. Candolin, *Security Issues for Wearable Computing and Bluetooth Technology*, 23 Oct. 2000, Telecommunications

2

Software and Multimedia Laboratory, Helsinki University of Technology, P.B. 400, FIN-02015 HUT, Finland, describes Bluetooth Technology as "a short-range wireless cable replacement technology enabling restricted types of ad hoc networks to be formed. All the while, a need for connecting wearable devices, such as PDAs, mobile phones, and mp3-players, is rising. Such networks may be formed using Bluetooth technology, but issues such as security must be taken into consideration. Although an attempt to tackle security is made, the result is too weak to be used for anything else than for personal purposes."

Other systems provide various details of the operation of wireless devices within a network, such as U.S. Pat. No. 6,418,324, Apparatus and Method for Transparent Wireless Communication; U.S. Pat. No. 6,418,146, Integrated Communication Center Functionality for WAP Devices; U.S. Pat. No. 6,359,880, Public Wireless/Cordless Internet Gateway; U.S. Pat. No. 6,334,056, Secure Gateway Processing for Handheld Device Markup Language; U.S. Pat. No. 6,317,594, System and Method for Providing Data to a Wireless Device Upon Detection of Activity of the Device on a Wireless Network; U.S. Pat. No. 6,282,183, Method for Authorizing Coupling between devices in a Capability Addressable Network; U.S. Pat. No. 6,272,129, Dynamic Allocation of Wireless Mobile Nodes Over An Internet Protocol (IP) Network; U.S. Pat. No. 6,167,428, Personal Computer Microprocessor Firewalls for Internet Distributed Processing; European Pat. No. 1225778, Wireless Repeater Using Identification of Call Originator; European Pat. No. EP 1191763, Access Authentication System for a Wireless Environment; European Pat. No. 1126681, A Network Portal System and Methods; European Pat. No. EP1081895, Secure Wireless Local Area Network; European Pat. No. EP 999672, System and Method for Mapping Packet Data Functional Entities to Elements in a Communications Network; European Pat. No. EP814623, Mobile Decision Methodology for Accessing Multiple Wireless Data Networks; *Privacy and Authentication for Wireless Local Area Networks*, Ashar Aziz and Whitfield Diffie; Sun Microsystems, Inc., Jul. 26, 1993; *Painting Your Home Blue (Bluetooth™ Wireless Technology)*, D. Cypher, Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances, Jan. 15–16, 2002; *Wireless Home Networks on a Hierarchical Bluetooth Scatternet Architecture*, W. Lilakiatsakun, A. Seneviratne, Proceedings Ninth IEEE International Conference on Networks; Oct. 10–12, 2001; *Bluetooth Wireless Technology in the Home*, R. Shephard, Electronics & Communication Engineering Journal; October 2001; *Wireless Gateway for Wireless Home AV Network and Its Implementation*, T. Saito, I. Imoda, Y. Takabatke, K. Teramoto, and K. Fujimoto, IEEE Transactions on Consumer Electronics, August 2001; *A Wireless Home Network and its Applications Systems*, H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura, IEEE Transactions on Consumer Electronics, May 2000; *Wireless Home Link*, M. Nakagawa, IEICE Transactions on Communications, December 1999; *An Access Protocol for a Wireless Home Network*, A. C. V. Gummalla, and J. O. Limb, WCNC 1999 IEEE Wireless Communications and Networking Conference; Sep. 21–24, 1999; *Firewalls for Security in Wireless Networks*, U. Murthy, O. Bukres, W. Winn, and E. Vanderdez, Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Jan. 6–9, 1998; *Self-Securing Ad Hoc Wireless Networks*, Haiyun Luo, Petros Aerfos, Jiejun Kng, Songwu Lu, and Lixia Zhang; *Wireless Networking for Control and Automation of Off-Road Equipment*, J. D. Will; ASAE Meeting Presentation;

US 6,891,807 B2

3

and *Intrusion Detection in Wireless Ad-Hoc Networks*, Yongguang Zhang and Wenke Lee, Proceeding of the Sixth Annual International Conference on Mobile Computing and Networking, Aug. 6–11, 2000.

The disclosed prior art systems and methodologies thus provide basic provisioning for wireless devices to a network through an access point. However, for many networks, such provisioning schemes are often impractical, either for wireless devices which lack a user interface which is configured for communicating provisioning information, or for simple home-based intranets. For example, device identification information, such as a MAC address, is often required to be manually transcribed from the wireless device to the access point, since wireless devices often lack a user interface control to reveal such identifying information. For example, a wireless picture frame device typically lacks a control interface to read or extract identification information, such as a MAC address.

While some wireless devices include a user interface for dedicated device functionality, e.g. such as a user control for a game box or a digital video recorder, a dedicated user interface is often incapable or cumbersome to be used to communicate device identification and to exchange provisioning information. In addition, while some wireless devices provide a user interface control which can reveal such identifying information, provisioning procedures still require a user to be technically proficient to properly initiate and complete a provisioning process.

It would therefore be advantageous to provide a network provisioning system, which does not require a user interface for the initiation of a provisioning process. The development of such a wireless access provisioning system would constitute a major technological advance.

Furthermore, it would be advantageous to provide a wireless access provisioning structure and process with minimal device requirements and/or user proficiency, whereby a wireless device is readily provisioned by the provisioning system, and whereby other devices within an access region are prevented from being provisioned by the provisioning system. The development of such a provisioning system would constitute a further technological advance.

As well, it would be advantageous that such a wireless access provisioning system be integrated with easily monitored parameters of a wireless device, such as the time monitoring of power on and/or start of signal transmission. The development of such a provisioning system would constitute a further major technological advance. The development of such a time-based wireless access provisioning system for provisioning secure encrypted communication would constitute a further technological advance.

### SUMMARY OF THE INVENTION

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter, such as the power on, of the wireless device occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

4

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic plan view of a time based wireless access provisioning system;

FIG. 2 is a functional block diagram of a time based wireless access provisioning system;

FIG. 3 is a flow chart of a time based wireless access provisioning process;

FIG. 4 is a flow chart of an alternate time based wireless access provisioning process;

FIG. 5 shows a simplified timeline for a time based wireless access provisioning process;

FIG. 6 shows a simplified timeline for an alternate time based wireless access provisioning process; and

FIG. 7 shows the time-based acceptance and provisioning of a new wireless device within a time based wireless access provisioning system.

### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 is a schematic plan view 10 of a time based wireless access provisioning system 20. FIG. 2 is a functional block diagram of a time based wireless access provisioning system 20, comprising a network access point 12 adapted to provide time-based provisioning with a wireless device 14.

The network access point 12 shown in FIG. 2 comprises a transceiver 32 and antenna 34, which provides communication 16 to one or more wireless devices 14. The communications channel 16 typically comprises an input, i.e. reverse link, signal 28 from a wireless device 14 to the access point, as well as an output, i.e. forward link, signal 30, from the access point 12 to the wireless device 14.

As seen in FIG. 2, the network access point 12 typically comprises network logic and componentry 36, such as networking functions 40, thereby providing communications between one or more authorized wireless devices 14 and a local network 17 (FIG. 1). The network access point 12 shown in FIG. 2 also comprises a network connection 38 to one or more networks 39, such as to wired devices within a LAN, and/or to other networks, such as the Internet. The network access point 12 shown in FIG. 2 comprises an access control list 42, which identifies wireless devices 14 which have proper access to the local network 17 (FIG. 1), such as by storing accepted device identifications 50 as list elements 43a–43n.

The wireless device 14 shown in FIG. 2 comprises a device transceiver 22 and antenna 24, which provides communication 16 to the network access point 12, and in some embodiments to other wireless devices 14. The wireless device 14 comprises communication logic and componentry 48, and comprises an associated device identifier 50, e.g. such as a unique MAC address, which is communicable to the network access point 12, whereby the wireless device 14 can be controllably provisioned into the network 17 by the network access point 12. The wireless device 14 also comprises power 26, e.g. wired or battery, and power activation 27. In some embodiments of the time based wireless access provisioning system 20, the wireless device 14 is an IEEE 802.11 WLAN and/or Bluetooth™ compliant device.

The network access point 12 shown in FIG. 1 is located within a service area 18 for a network 17, such as a wireless local area network (WLAN) or a wireless personal area network (WPAN), and typically communicates 16 with a one or more wireless devices 14 which operate within the

US 6,891,807 B2

5

service area 18, as well as to other wired devices connected to the network, and to connected 38 networks 39, such as the Internet.

As seen in FIG. 1, the time based wireless access provisioning system 20 can be used for a wide variety of wireless devices 14a-14n which are adapted to communicate with the network access point 12, such as but not limited to a desktop computer 14a, a portable laptop computer 14b, a network printer 14c, a digital video recorder 14d, a game box 14e, a portable phone 14f, a personal digital assistant (PDA) 14g, and/or a wireless picture frame 14h.

The network access point 12 provides time-based provisioning to ensure that only authorized wireless devices 14 can operate within the local network 17, such as within a home HM, and to prevent unauthorized wireless devices 14, such as device 14n in FIG. 1, from gaining access to the network 17.

In the time based wireless access provisioning system 20, the network access point 12 also comprises time based provisioning 44, which is activatable 46, such as manually by a user U. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17. A properly timed interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12 acts to qualify the wireless device 14 to the network access point. Time-Based Provisioning Process.

FIG. 3 is a flow chart of a time based wireless access provisioning process 52a. The network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 5). The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46.

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 3, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, e.g. such as within 5 minutes. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 5), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 3, the time based wireless access provisioning process 52a also prevents network access from devices 14 which are powered on 78 (FIG. 5) at an earlier time 88 (FIG. 5). If a wireless device 14 is powered on at a time 88 before the acceptance time interval 74 (FIG. 5), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device, preventing provisioning 64 into the network 17.

FIG. 5 shows a simplified timeline 70a for a time based wireless access provisioning process 52a. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 5, the network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. The user then activates provisioning logic 44 at the network access point 12, at time 86. The provisioning logic 44 typically comprises an acceptance time interval 74, e.g. such as a 5 minute interval 74, having a start time 84 and an end time 86, within which desired devices 14 are accepted 62 (FIG. 3). As seen in FIG. 5, the time interval 76 for the desired device 14 properly falls

6

within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 5, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12. When the user activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, i.e. failing 66 time-based determination 60 (FIG. 3) such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Alternate Time-Based Provisioning Process.

FIG. 4 is a flow chart of an alternate time based wireless access provisioning process 52b, in which a desired wireless device 14 to be provisioned is powered on after the provisioning logic 44 is activated. As above, the network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 6).

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 4, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, after the provisioning logic 44 is activated 58. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 6), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 4, the alternate time based wireless access provisioning process 52b also prevents network access from devices 14 which are powered on 78 (FIG. 6) at an earlier time 88 (FIG. 6). If a wireless device 14 is powered on at a time 88 before (or after) the acceptance time interval 74 (FIG. 6), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device 14, preventing provisioning 64 into the network 17.

FIG. 6 shows a simplified timeline 70b for the alternate time based wireless access provisioning process 52b. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 6, the user activates provisioning logic 44 at the network access point 12, at time 84. The network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. If the power on 56 falls within the acceptance time interval 74, the desired device 14 is accepted 62 (FIG. 4). As seen in FIG. 6, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 6, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12, such as from an unauthorized device 14, or from a desired device which is not powered on within the time interval 74. When the user then activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, and before the activation 58 of the provisioning logic 44,



US 6,891,807 B2

7

such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Device Qualification.

FIG. 7 provides a schematic view 90 of a time-based acceptance of a new wireless device 14 within a time based wireless access provisioning system 20.

When the provisioning logic 44 time-qualifies 62 (FIG. 3, FIG. 4) a wireless device 14, the wireless access point 12 accepts the time-based qualification 57, and initiates the provisioning process 64, which typically comprises communication 16 and secure provisioning of information between the wireless device 14 and the network access point 12, such as the exchange of key material, if an encryption protocol is to be used. Device parameters, such as the device identifier 50, are typically sent 92 to the access point 12, wherein the device identifier 50 is added to the network access control list 42. As seen in FIG. 7, the device identifier 50 for the accepted wireless device 14 is added to the access control list 42, such as an element 43b in the list of qualified devices 14. Provisioning information may also be sent 94 from the network access point 12 to the device 14, such as to establish setup, handshaking, or encryption provisioning.

System Implementation.

The time-based wireless access provisioning system 20 readily integrates one or more wireless devices 14 into a local area network in a secure fashion. For example, when a user U brings home a new wireless device 14 for use in their existing home network 17, the time-based wireless access provisioning system 20 allows the user U to easily add the new device to the network 17, without exposing the network unnecessarily to attack from third parties.

Within the time based access provisioning system 20, the enhanced network access point 12 keeps track of all wireless devices 14a-14n in the vicinity 18 of the central access point 12. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17, based upon a properly timed device qualification interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12.

As seen in FIG. 3 and FIG. 4, when a user U brings a device 14 home HM and powers on the wireless device 14, the user then simply presses a button 46 on their network access point 12. In response thereto, the access point 12 provisions the wireless device automatically, based on the time-based qualification 57. Since the access point 12 is only available for such provisioning for a short interval 74 after the button 46 is pressed, it is unlikely that the access point 12 will provision unauthorized third party devices 14.

The qualification protocol 52a,52b allows the network access point 12 to augment the access control list 42 with a properly qualified device 14. The network access point can discount, i.e. deny, devices in neighboring residences HM that have been on for a long time, wherein power on 78 of the devices 14 extends beyond the acceptance interval 74, and can identify and provision one or more devices 14 that are powered on 56 within the acceptance interval 74.

The time-based access provisioning system 20 does not require a user interface on a wireless device 14 to initiate device setup and provisioning. As the power on or beginning of signal transmission 16 is easily tracked by the enhanced network access point 12, a simple activation 46, such as the pushing of a button 46, can be used to time-qualify 57 a desired device 14, and to deny qualification 66 for an unqualified device. Therefore, the time-based access provisioning system 20 drastically simplifies wireless setup and provisioning for wireless devices. Wireless devices 14 to be

8

provisioned are not required to have complex user interfaces, and users are not required to perform complex provisioning procedures. The time-based access provisioning system 20 simplifies the integration of wireless devices into a network, and provides more than reasonable levels of security.

Alternate Applications for the Time-Based Access Provisioning System.

While the time based access provisioning system 10 is disclosed above as tracking a single power on 56,78 of wireless devices, alternate embodiments of the time based access provisioning system 10 provide further network protections from undesired devices.

For example, for a neighboring device which is switched on and off repeatedly, such as for an undesired wireless device or user in search of a network access point 12, the network access point 12 tracks the repeated powering operation, and can deny provisioning access as desired.

Although the time based access provisioning system and its methods of use are described herein in connection with wireless devices, personal computers and other microprocessor-based devices, such as wireless appliances, the apparatus and techniques can be implemented for a wide variety of electronic devices and systems, or any combination thereof, as desired.

Furthermore, while the time based access provisioning system and its methods of use are described herein in connection with wireless devices and intranets or LAN's, the apparatus and techniques can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

As well, while the time based access provisioning system and its methods of use are described herein in connection with a time based interaction between a wireless device and a network access point, the use of tracking power on/off as a signal to associate devices automatically can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.

What is claimed is:

1. A process for provisioning between a wireless device and a network, comprising the steps of:

providing an access point connected to the network, the access point comprising logic for determining the power on time of the wireless device;  
powering on the wireless device;  
activating a time interval; and  
initiating provisioning with the wireless device if the power on of the wireless device occurs within the time interval.

2. The process of claim 1, wherein the wireless device is any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

3. The process of claim 1, wherein the wireless device is an IEEE 802.11 compliant device.

4. The process of claim 1, wherein the wireless device is a BLUETOOTH™ compliant device.

5. The process of claim 1, wherein the network is a local area network.



US 6,891,807 B2

9

6. The process of claim 1, wherein the network is a wireless local area network.

7. The process of claim 1, wherein the network is connected to the Internet.

8. The process of claim 1, further comprising the step of: preventing provisioning with the wireless device if the power on of the wireless device is greater than the time interval.

9. The process of claim 1, wherein the access point comprises an access control list comprising storage for a device identifier corresponding to a wireless device which is provisioned to access the network.

10. The process of claim 9, wherein the device identifier is a MAC address.

11. The process of claim 1, wherein the provisioning comprises associating a received device identifier with the wireless device.

12. The process of claim 1, wherein the provisioning comprises storing a MAC address from the wireless device.

13. The process of claim 1, wherein the provisioning comprises a communication of an access control list to the wireless device.

14. The process of claim 1, wherein the wireless device further comprises a device identifier, and wherein the provisioning comprises communicating the device identifier to the access point.

15. The process of claim 1, wherein the provisioning comprises establishing an encrypted connection between the wireless device and the network.

16. The process of claim 1, wherein the provisioning comprises an established connection between the wireless device and at least one other provisioned wireless device.

17. A time based network access provisioning system between a wireless device and a network, comprising:

a network access point connected to the network, the network access point comprising logic for tracking operation of the wireless device; and

logic for provisioning the wireless device if the operation of the wireless device occurs within an activatable time interval.

18. The system of claim 17, wherein the wireless device is any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

19. The system of claim 17, wherein the wireless device is an IEEE 802.11 compliant device.

20. The system of claim 17, wherein the wireless device is a BLUETOOTH™ compliant device.

21. The system of claim 17, wherein the network is a local area network.

22. The system of claim 17, wherein the network is a wireless local area network.

23. The system of claim 17, wherein the network is connected to the Internet.

24. The system of claim 17, further comprising: logic for preventing provisioning with the wireless device if the power on of the wireless device is greater than the time interval.

25. The system of claim 17, wherein the access point comprises an access control list comprising storage for a device identifier corresponding to a wireless device which is provisioned to access the network.

26. The system of claim 25, wherein the device identifier is a MAC address.

27. The system of claim 17, wherein the provisioning logic comprises an association of a received device identifier with the wireless device.

10

28. The system of claim 17, wherein the provisioning logic comprises means for storing a MAC address associated with the wireless device.

29. The system of claim 17, wherein the provisioning logic comprises a communication of an access control list to the wireless device.

30. The system of claim 17, wherein the provisioning logic comprises an established encrypted connection between the wireless device and the network.

31. The system of claim 17, wherein the provisioning comprises establishing an encrypted connection between the wireless device and the network.

32. The system of claim 17, wherein the provisioning logic comprises an established connection between the wireless device and at least one other provisioned wireless device.

33. A process for provisioning between a wireless device and a network, comprising the steps of:

providing an access point connected to the network, the access point comprising logic for determining the time of power on of the wireless device;

determining of the wireless device is powered within a specified interval; and

initiating provisioning of the wireless device if the power occurs within the interval.

34. The process of claim 33, wherein the wireless device is any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

35. The process of claim 33, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

36. The process of claim 33, wherein the network comprises any of a local area network and a wireless local area network.

37. The process of claim 33, wherein the network is connected to the Internet.

38. The process of claim 33, further comprising the step of:

preventing provisioning with the wireless device if the power on of the wireless device is greater than the time interval.

39. The process of claim 33, wherein the access point comprises an access control list comprising storage for a device identifier corresponding to at least one wireless device which is provisioned to access the network.

40. The process of claim 39, wherein the device identifier is a MAC address.

41. The process of claim 33, wherein the provisioning comprises associating a received device identifier with the wireless device.

42. The process of claim 33, wherein the provisioning comprises a communication of an access control list to the wireless device.

43. The process of claim 33, wherein the wireless device further comprises a device identifier, and wherein the provisioning comprises communicating the device identifier to the access point.

44. The process of claim 33, wherein the provisioning comprises establishing an encrypted connection between the wireless device and the network.

45. The process of claim 33, wherein the provisioning comprises an established connection between the wireless device and at least one other provisioned wireless device.

46. A process for provisioning between a wireless device and a network, the wireless device having a transmitted signal, comprising the steps of:

US 6,891,807 B2

11

providing an access point connected to a network, the access point comprising an activatable provisioning time interval; and

initiating provisioning of the wireless device if the transmission of the wireless signal from the wireless device to the access point begins during the interval.

47. The process of claim 46, wherein the wireless device is any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

48. The process of claim 46, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

49. The process of claim 46, wherein the network comprises any of a local area network and a wireless local area network.

50. The process of claim 46, wherein the network is connected to the Internet.

51. The process of claim 46, further comprising the step of:

preventing provisioning with the wireless device if the transmission of the wireless device signal begins outside of the time interval.

52. The process of claim 46, wherein the access point comprises an access control list comprising storage for a device identifier corresponding to at least one wireless device which is provisioned to access the network.

53. The process of claim 52, wherein the device identifier is a MAC address.

54. The process of claim 46, wherein the provisioning comprises associating a received device identifier with the wireless device.

55. The process of claim 46, wherein the provisioning comprises a communication of an access control list to the wireless device.

56. The process of claim 46, wherein the wireless device further comprises a device identifier, and wherein the provisioning comprises communicating the device identifier to the access point.

57. The process of claim 46, wherein the provisioning comprises establishing an encrypted connection between the wireless device and the network.

58. The process of claim 46, wherein the provisioning comprises an established connection between the wireless device and at least one other provisioned wireless device.

59. A network access point, comprising:

a connection to a network;

a receiver for receiving input signals from at least one wireless device;

12

means for provisioning access between the wireless device and the network; and

a time-based interval which selectably allows the provisioning if a received input signal occurs within the time interval.

60. The network access point of claim 59, wherein the wireless device is any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

61. The network access point of claim 59, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

62. The network access point of claim 59, wherein the network comprises any of a local area network and a wireless local area network.

63. The network access point of claim 59, wherein the network is connected to the Internet.

64. The network access point of claim 59, further comprising:

logic for preventing provisioning with the wireless device if the power on of the wireless device is greater than the time interval.

65. The network access point of claim 59, wherein the access point comprises an access control list comprising storage for a device identifier corresponding to a wireless device which is provisioned to access the network.

66. The network access point of claim 64, wherein the device identifier is a MAC address.

67. The network access point of claim 59, wherein the provisioning means comprises an association of a received device identifier with the wireless device.

68. The network access point of claim 59, wherein the provisioning means comprises a communication of an access control list to the wireless device.

69. The network access point of claim 59, wherein the wireless device further comprises a device identifier, and wherein the provisioning means comprises a communication of the device identifier to the access point.

70. The network access point of claim 59, wherein the provisioning means comprises an established encrypted connection between the wireless device and the network.

71. The network access point of claim 59, wherein the provisioning means comprises an established connection between the wireless device and at least one other provisioned wireless device.

\* \* \* \* \*

# Exhibit G

---



US007177285B2

(12) **United States Patent**  
**Roskind et al.**

(10) **Patent No.:** **US 7,177,285 B2**  
(45) **Date of Patent:** **\*Feb. 13, 2007**

(54) **TIME BASED WIRELESS ACCESS  
PROVISIONING**

6,167,428 A 12/2000 Ellis ..... 709/201  
6,272,129 B1 8/2001 Dynarski et al. .... 370/356  
6,275,693 B1 8/2001 Lin et al. .... 455/414

(75) Inventors: **James A. Roskind**, Redwood City, CA  
(US); **John D. Robinson**, South Riding,  
VA (US)

(Continued)

#### FOREIGN PATENT DOCUMENTS

(73) Assignee: **America Online, Incorporated**, Dulles,  
VA (US)

EP 814 623 12/1997

(Continued)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 188 days.

#### OTHER PUBLICATIONS

*Security Issues for Wearable Computing and Bluetooth Technology*;  
Catharina Candolin, undated.

(Continued)

(21) Appl. No.: **10/961,959**

*Primary Examiner*—Melvin Marcelo

(22) Filed: **Oct. 8, 2004**

(74) *Attorney, Agent, or Firm*—Michael A. Glenn; Glenn  
Patent Group

(65) **Prior Publication Data**

US 2005/0043021 A1 Feb. 24, 2005

#### Related U.S. Application Data

(63) Continuation of application No. 10/341,847, filed on  
Jan. 13, 2003, now Pat. No. 6,891,807.

(51) **Int. Cl.**

**H04L 12/26** (2006.01)

**H04Q 7/34** (2006.01)

(52) **U.S. Cl.** ..... 370/255; 370/338

(58) **Field of Classification Search** ..... 370/255,  
370/338

See application file for complete search history.

(56) **References Cited**

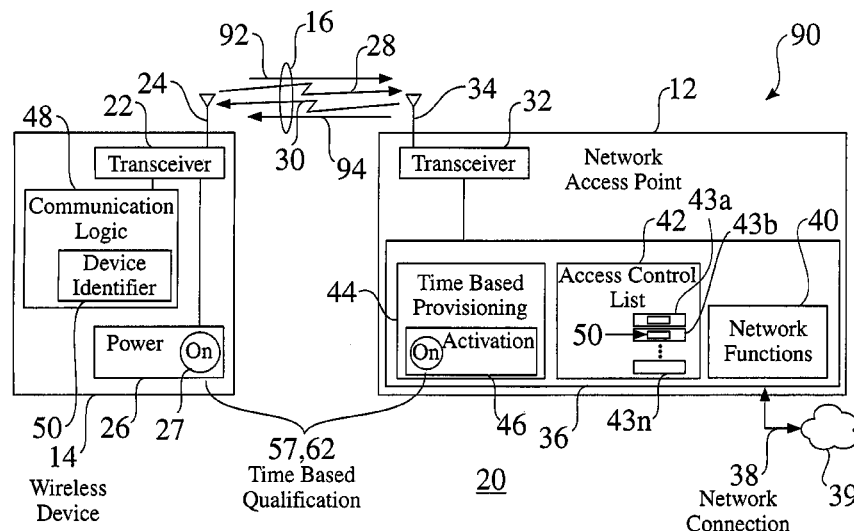
#### U.S. PATENT DOCUMENTS

5,461,627 A \* 10/1995 Rypinski ..... 370/346  
6,058,106 A 5/2000 Cudak et al. .... 370/313

(57) **ABSTRACT**

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter (such as power on or the onset of signal transmission) of the wireless device occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. In one system embodiment, the network access point tracks the power on time of wireless devices. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

**62 Claims, 7 Drawing Sheets**



## US 7,177,285 B2

Page 2

## U.S. PATENT DOCUMENTS

6,282,183	B1	8/2001	Harris et al. ....	370/338
6,317,594	B1	11/2001	Gossman et al. ....	455/414
6,334,056	B1	12/2001	Holmes et al. ....	455/445
6,359,880	B1	3/2002	Curry et al. ....	370/352
6,418,146	B1	7/2002	Miloslavsky ....	370/400
6,418,324	B1	7/2002	Doviak et al. ....	455/556
6,891,807	B2 *	5/2005	Roskind et al. ....	370/255
2001/0048744	A1 *	12/2001	Kimura ....	380/247
2003/0152235	A1 *	8/2003	Cohen et al. ....	380/278

## FOREIGN PATENT DOCUMENTS

EP	999 672	5/2000
EP	1 081 895	3/2001
EP	1 126 681	8/2001
EP	1 191 763	3/2002
EP	1 225 778	7/2002
JP	2001-308866	11/2001
WO	WO 01/22661	3/2001

## OTHER PUBLICATIONS

*Privacy and Authentication for Wireless Local Area Networks*; Ashar Aziz, and Whitfield Diffie; Sun Microsystems, Inc.; Jul. 26, 1993.

*Painting Your Home Blue [Bluetooth/sup TM/wireless Technology]*; D. Cypher; Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances; Jan. 15-16, 2002.

*Wireless Home Networks Based on a Hierarchical Bluetooth Scatternet Architecture*; W. Lilakiatsakun, A. Seneviratne; Proceedings Ninth IEEE International Conference on Networks; Oct. 10-12, 2001.

*Bluetooth Wireless Technology in the Home*; R. Sheperd; Electronics & Communication Engineering Journal; Oct. 2001.

*Wireless Gateway for Wireless Home AV Network and Its Implementation*; T. Saito, I. Imoda, Y. Takabatke, and K. Teramoto, and K. Fujimoto; IEEE Transactions on Consumer Electronics; Aug. 2001.

*A Wireless Home Network and Its Application Systems*; H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura; IEEE Transactions on Consumer Electronics; May 2000.

*Wireless Home Link*; M. Nakagawa; IEICE Transactions on Communications; Dec. 1999.

*An Access Protocol for a Wireless Home Network*; A.C.V. Gummalla, and J.O. Limb; WCNC. 1999 IEEE Wireless Communications and Networking Conference; Sep. 21-24, 1999.

*Firewalls for Security in Wireless Networks*; U. Murthy, O. Bukhres, W. Winn, and E. Vanderdez; Proceedings of the Thirty-First Hawaii International Conference on System sciences; Jan. 6-9, 1998.

*Self-Securing Ad Hoc Wireless Networks*; Haiyun Luo, Petros Aefos, Jiejun Kng, Songwu Lu, and Lixia Zhang, undated.

*Wireless Networking for Control and Automation of Off-Road Equipment*; by J.D. Will; An ASAE Meeting Presentation, undated.

*Intrusion Detection in Wireless Ad-Hoc Networks*; Yongguang Zhang and Wenke Lee; Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking; Aug. 6-11, 2000.

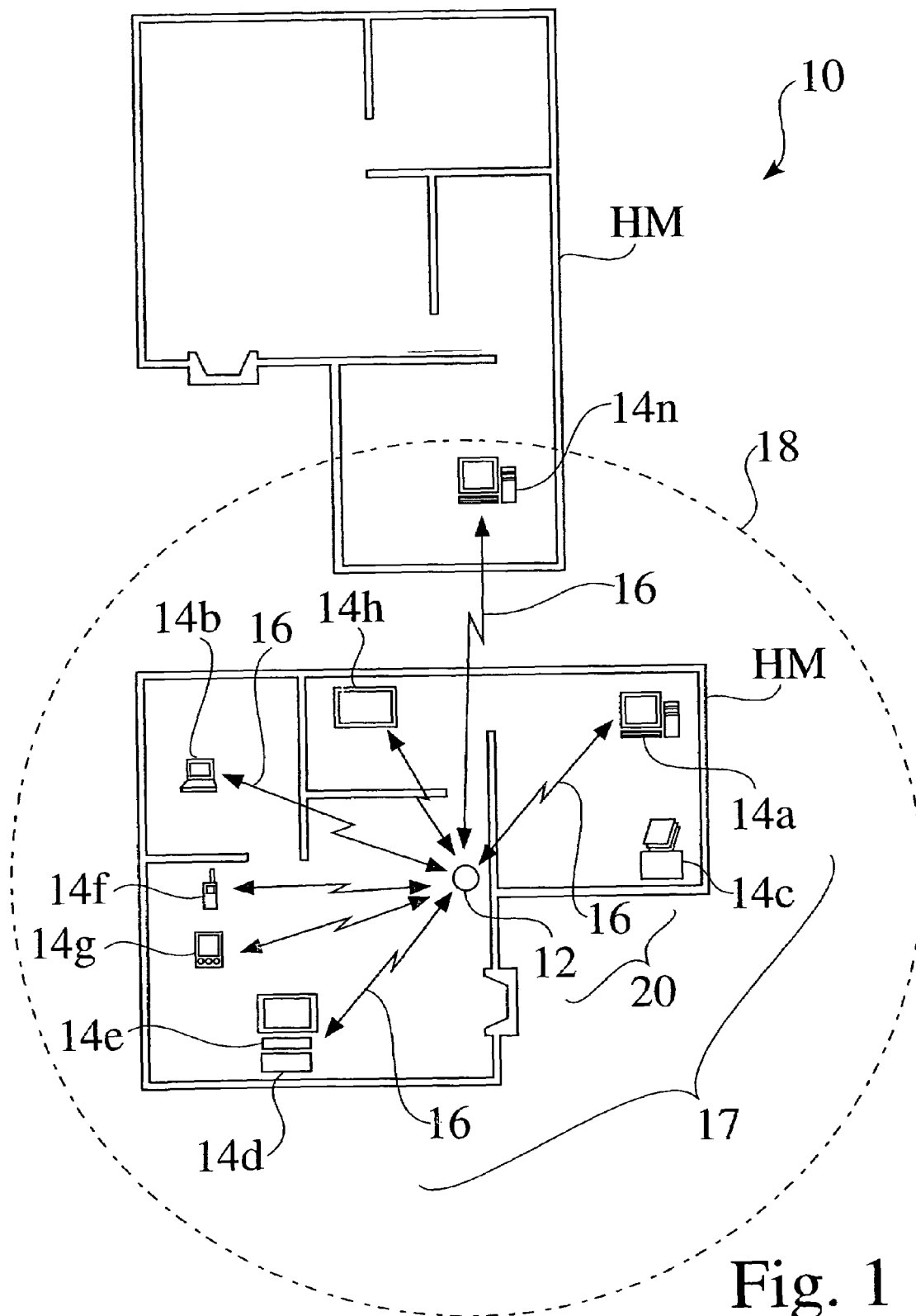
*Microsoft Announces Wireless Provisioning Services*; GeekZone; Wi-Fi, posted Dec. 10, 2003 20:56:21 NZ.

*HP Spotlights Mobile Gear*; Ina Fried; CNET News.com; Oct. 13, 2003.

*Wireless Provisioning Services Overview*; The Cable Guy—Dec. 2003; TechNet Newsletter; 2004 Microsoft Corporation.

Sony Ericsson Mobile Communications; *Sony Ericsson HBH-65* (Manual); Pub #LZT 1086746 R1A; 1<sup>st</sup> Ed. Aug. 2003; Sony Ericsson Mobile Communications, AB.

\* cited by examiner





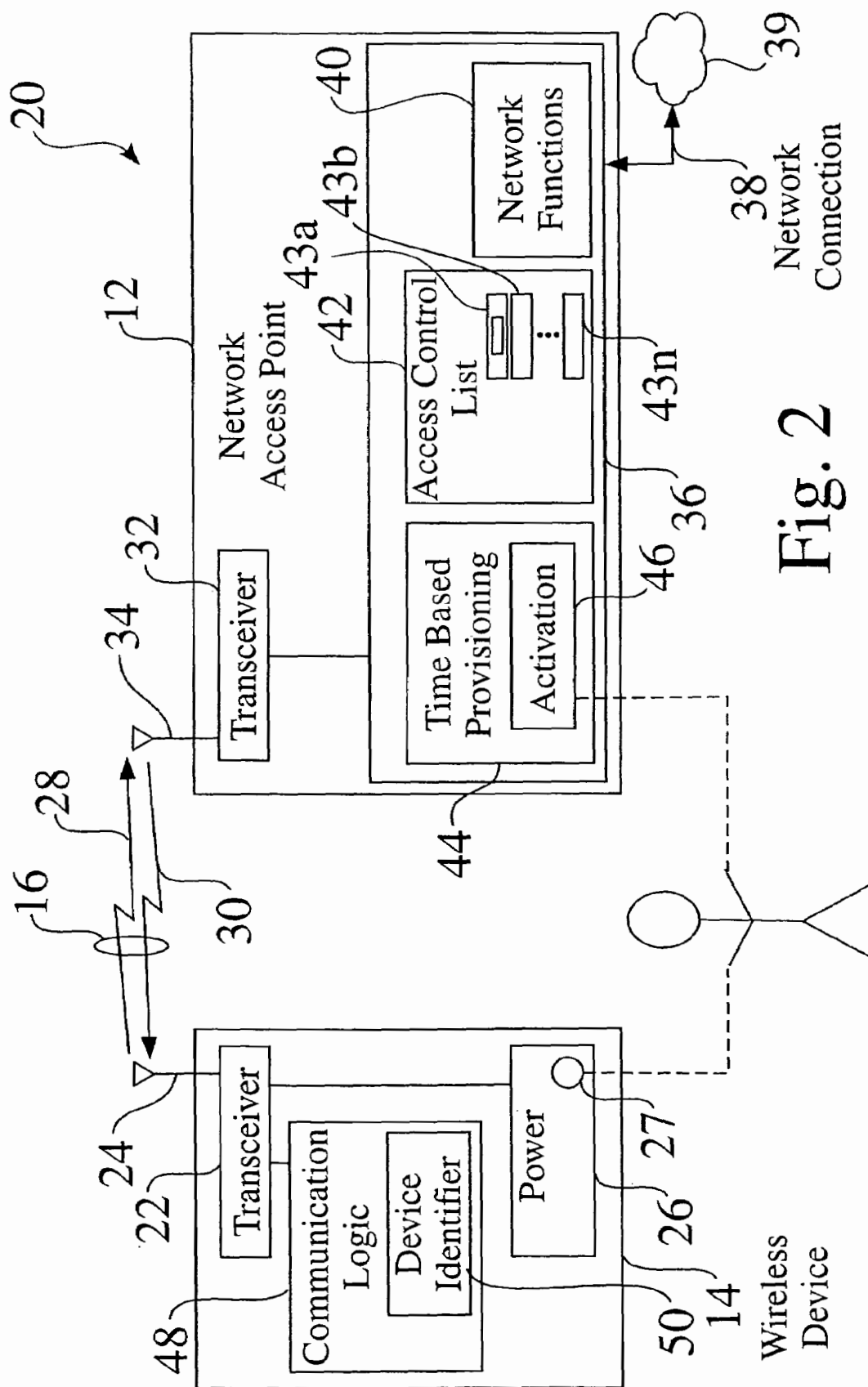


Fig. 2

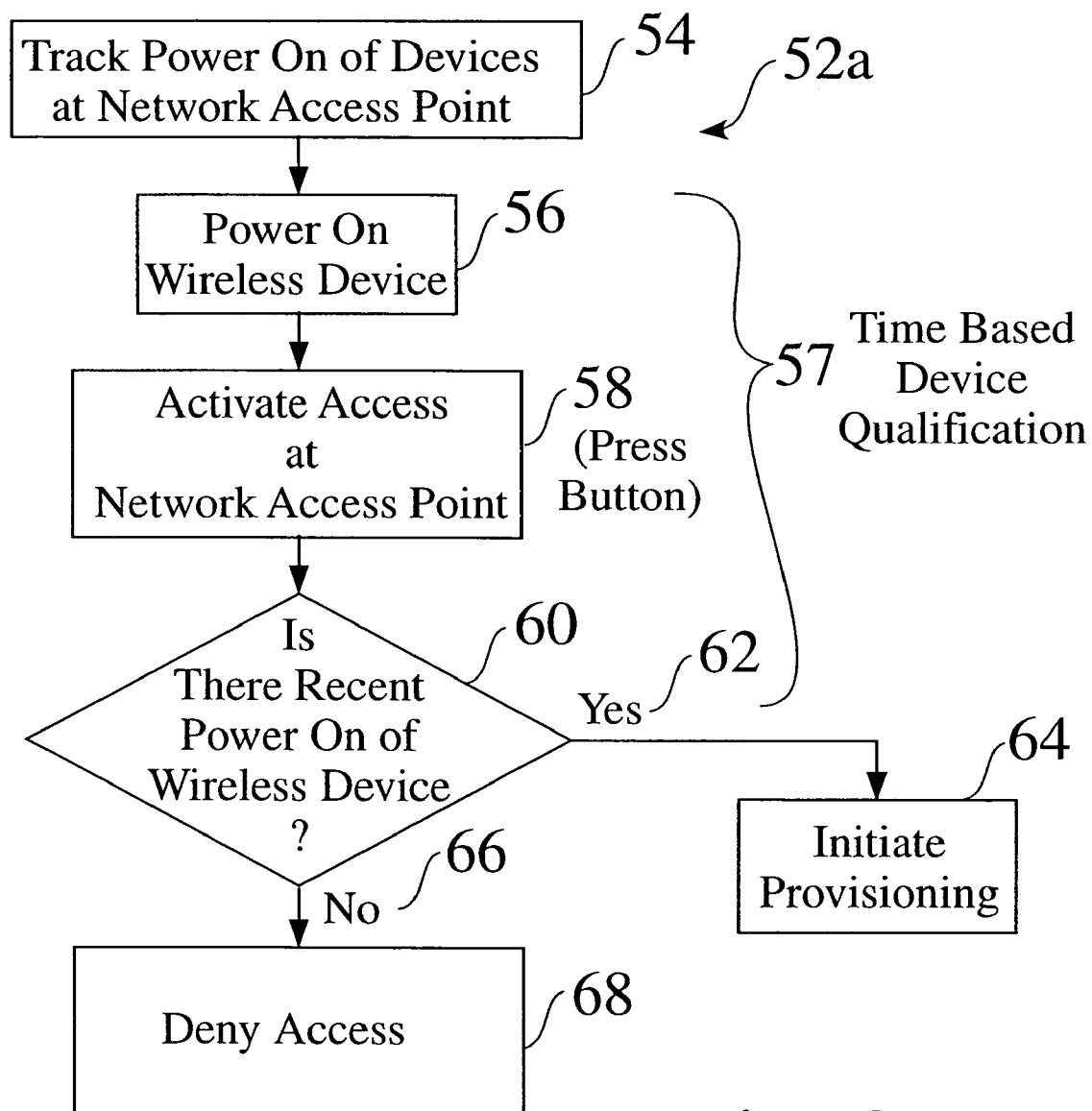


Fig. 3

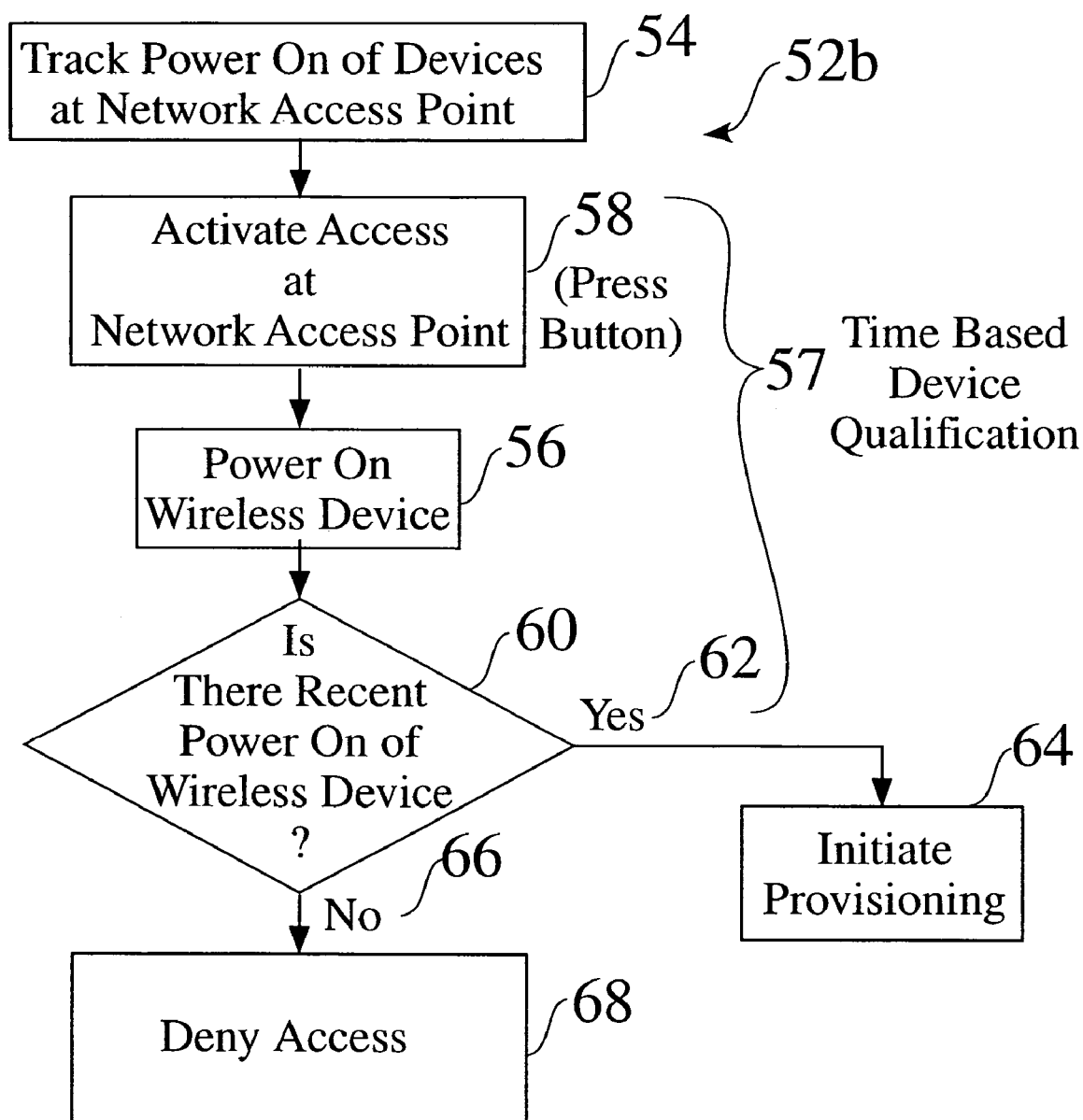


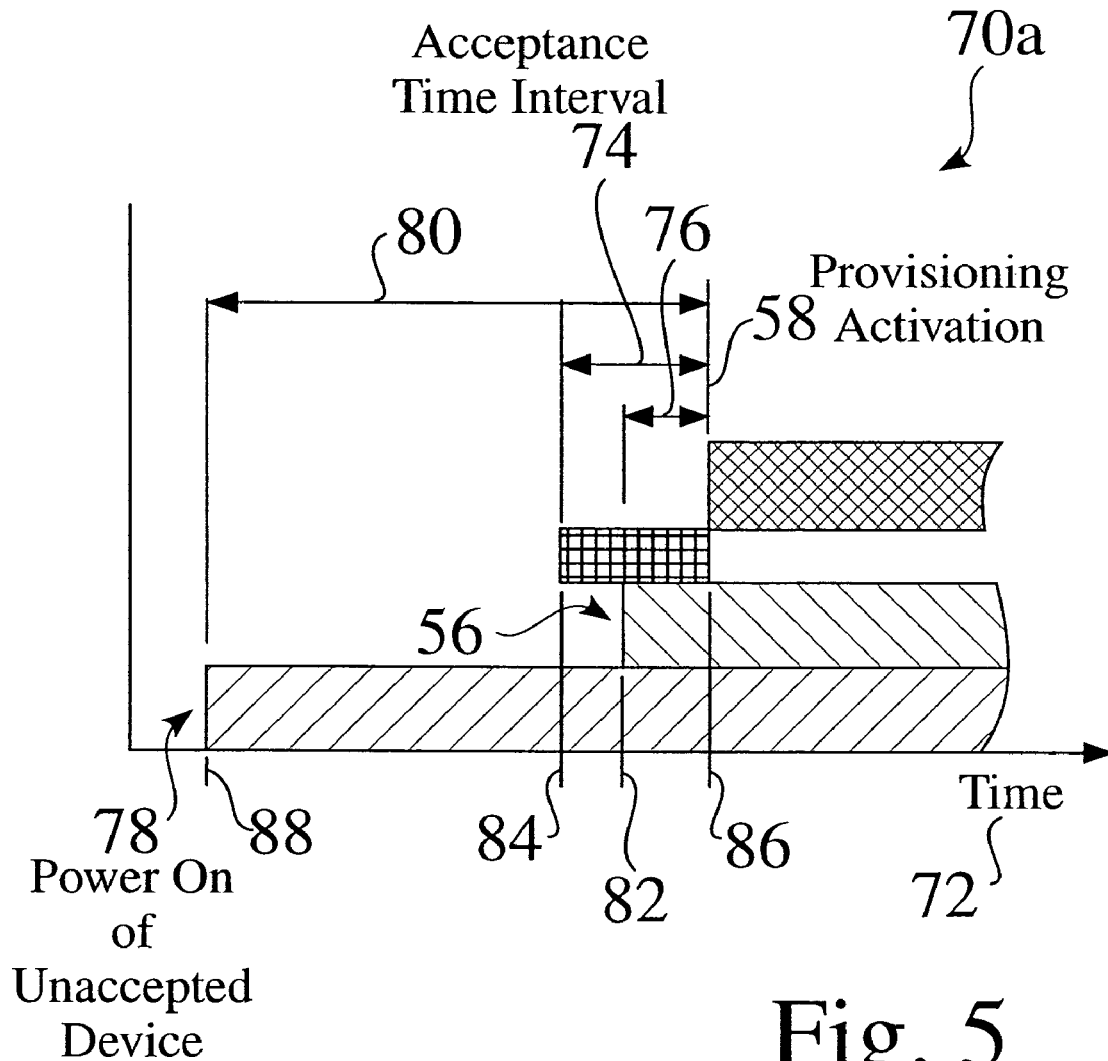
Fig. 4

U.S. Patent

Feb. 13, 2007

Sheet 5 of 7

US 7,177,285 B2



U.S. Patent

Feb. 13, 2007

Sheet 6 of 7

US 7,177,285 B2

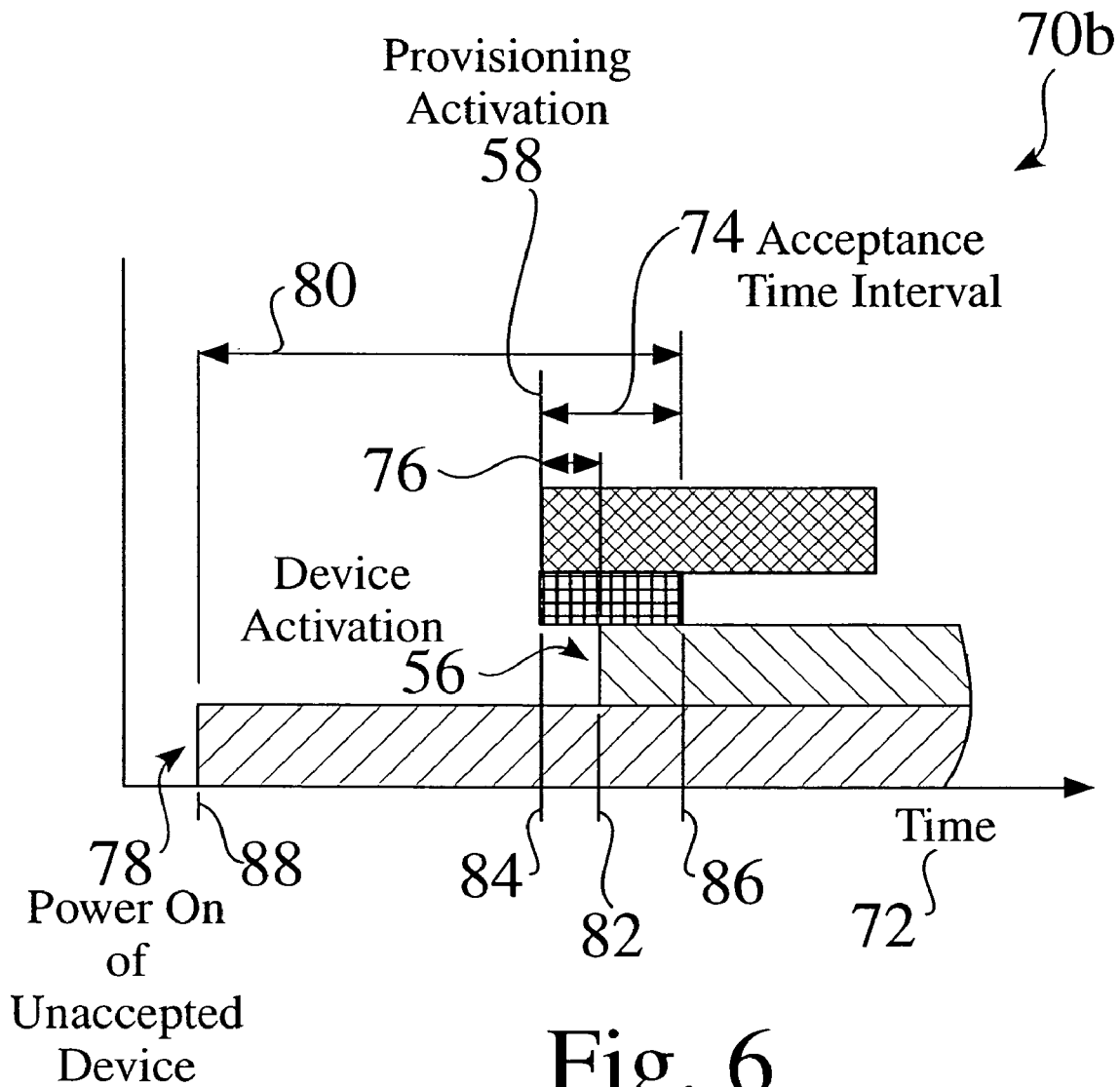
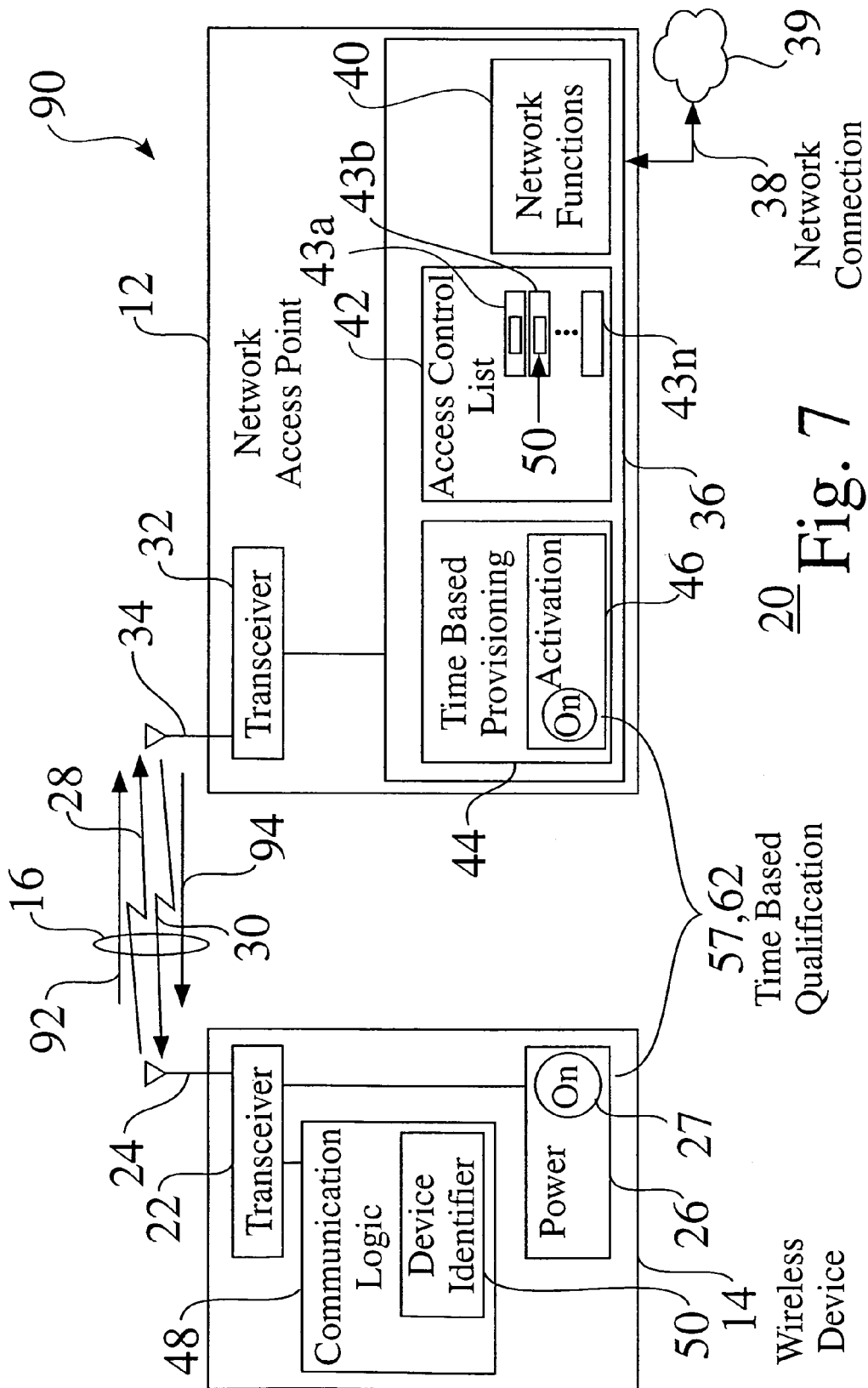


Fig. 6





US 7,177,285 B2

1

**TIME BASED WIRELESS ACCESS  
PROVISIONING****CROSS-REFERENCE TO RELATED  
APPLICATION**

This application is a continuation of U.S. Ser. No. 10/341,847, filed Jan. 13, 2003, now U.S. Pat. No. 6,891,807 B2, which is incorporated herein in its entirety by this reference thereto.

**FIELD OF THE INVENTION**

The invention relates to the field of wireless connections between a wireless device and a network. More particularly, the invention relates to access provisioning between one or more wireless devices and an intranet access point.

**BACKGROUND OF THE INVENTION**

In local area networks, such as wireless home networks, one or more wireless devices, e.g. such as IEEE 802.11b devices, are linked to the network by a provisioning process through a network access point. When a user acquires a new wireless device, they need to securely tie it to their intranet, which comprises telling the intranet to accept wireless communications from the device, as well as provisioning the device with key material, such as for creating an encrypted connection. In conventional networks having one or more devices to be provisioned to a network access point, device identification information, such as a MAC address, is required to be communicated from the wireless device to the access point.

Several methods have been described for wireless access provisioning to integrate wireless devices into a network.

M. Cudak, B. Mueller, J. Kelton, and B. Classon, Network Protocol Method, Access Point Device and Peripheral Devices for Providing for an Efficient Centrally Coordinated Peer-to-Peer Wireless Communications Network, U.S. Pat. No. 6,058,106, discloses a "peer-to-peer wireless communications network wherein the access point device: (1) broadcasts a block assignment that specifies a wireless source peripheral device and a wireless destination peripheral device; (2) receives, from the wireless destination peripheral device, sequence information; (3) determines whether the sequence information represents one of: a negative acknowledgment and a positive acknowledgment with a sequence number; (4) forwards an acknowledgment to the wireless source peripheral based on the sequence information, and repeats steps (1)–(4) until N blocks of data, N a predetermined integer, have been transferred from the wireless source peripheral to the wireless destination peripheral."

J. Lin, P. Alfano, and S. Upp, Method and Apparatus for Performing Bearer Independent Wireless Application Service Provisioning, U.S. Pat. No. 6,275,693 disclose a provisioning system, in which a "mobile communication device contacts a provisioning proxy over the wireless bearer network, which in turns contacts a provisioning center over a public network. A provisioning tunnel is then established between the provisioning center and the mobile communication device. Once the provisioning tunnel is set up, the user of the mobile communication device can subscribe to, or unsubscribe from wireless application services."

Wireless Device Registering Method in Wireless Home Network, PCT Patent Application No. WO 01/2266, describes the sending of an authentication key to a device for

2

storage, when an identification code received from the device corresponds to a code stored in an access point.

Secure Wireless LAN, European Pat. No. EP, 1081895, discloses wireless device use by a wireless device operator with an access point connected to a wired LAN in communication with the wireless device through air channel authentication.

C. Candolin, Security Issues for Wearable Computing and Bluetooth Technology, 23 Oct. 2000, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, P.B. 400, FIN-02015 HUT, Finland, describes Bluetooth Technology as "a short-range wireless cable replacement technology enabling restricted types of ad hoc networks to be formed. All the while, a need for connecting wearable devices, such as PDAs, mobile phones, and mp3-players, is rising. Such networks may be formed using Bluetooth technology, but issues such as security must be taken into consideration. Although an attempt to tackle security is made, the result is too weak to be used for anything else than for personal purposes."

Other systems provide various details of the operation of wireless devices within a network, such as U.S. Pat. No. 6,418,324, Apparatus and Method for Transparent Wireless Communication; U.S. Pat. No. 6,418,146, Integrated Communication Center Functionality for WAP Devices; U.S. Pat. No. 6,359,880, Public Wireless/Cordless Internet Gateway; U.S. Pat. No. 6,334,056, Secure Gateway Processing for Handheld Device Markup Language; U.S. Pat. No. 6,317,594, System and Method for Providing Data to a Wireless Device Upon Detection of Activity of the Device on a Wireless Network; U.S. Pat. No. 6,282,183, Method for Authorizing Coupling between devices in a Capability Addressable Network; U.S. Pat. No. 6,272,129, Dynamic Allocation of Wireless Mobile Nodes Over An Internet Protocol (IP) Network; U.S. Pat. No. 6,167,428, Personal Computer Microprocessor Firewalls for Internet Distributed Processing; European Pat. No. 1225778, Wireless Repeater Using Identification of Call Originator; European Pat. No. EP 1191763, Access Authentication System for a Wireless Environment; European Pat. No. 1126681, A Network Portal System and Methods; European Pat. No. EP1081895, Secure Wireless Local Area Network; European Pat. No. EP 999672, System and Method for Mapping Packet Data Functional Entities to Elements in a Communications Network; European Pat. No. EP814623, Mobile Decision Methodology for Accessing Multiple Wireless Data Networks; *Privacy and Authentication for Wireless Local Area Networks*, Ashar Aziz and Whitfield Diffie, Sun Microsystems, Inc., Jul. 26, 1993; *Painting Your Home Blue (Bluetooth™ Wireless Technology)*, D. Cypher, Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances, Jan. 15–16, 2002; *Wireless Home Networks on a Hierarchical Bluetooth Scatternet Architecture*, W. Lilakiatsakun, A. Seneviratne, Proceedings Ninth IEEE International Conference on Networks; Oct. 10–12, 2001; *Bluetooth Wireless Technology in the Home*, R. Shephard, Electronics & Communication Engineering Journal; October 2001; *Wireless Gateway for Wireless Home AV Network and It's Implementation*, T. Saito, I. Imoda, Y. Takabatke, K. Teramoto, and K. Fujimoto, IEEE Transactions on Consumer Electronics, August 2001; *A Wireless Home Network and its Applications Systems*, H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura, IEEE Transactions on Consumer Electronics, May 2000; *Wireless Home Link*, M. Nakagawa, IEICE Transactions on Communications, December 1999; *An Access Protocol for a Wireless Home Network*, A. C. V. Gummalla, and J. O. Limb, WCNC 1999 IEEE Wireless Communications

US 7,177,285 B2

3

and Networking Conference; Sep. 21–24, 1999; *Firewalls for Security in Wireless Networks*, U. Murthy, O. Bukres, W. Winn, and E. Vanderdez, Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Jan. 6–9, 1998; *Self-Securing Ad Hoc Wireless Networks*, Haiyun Luo, Petros Aerfos, Jiejun Kng, Songwu Lu, and Lixia Zhang; *Wireless Networking for Control and Automation of Off-Road Equipment*, J. D. Will; ASAE Meeting Presentation; and *Intrusion Detection in Wireless Ad-Hoc Networks*, Yongguang Zhang and Wenke Lee, Proceeding of the Sixth Annual International Conference on Mobile Computing and Networking, Aug. 6–11, 2000.

The disclosed prior art systems and methodologies thus provide basic provisioning for wireless devices to a network through an access point. However, for many networks, such provisioning schemes are often impractical, either for wireless devices which lack a user interface which is configured for communicating provisioning information, or for simple home-based intranets. For example, device identification information, such as a MAC address, is often required to be manually transcribed from the wireless device to the access point, since wireless devices often lack a user interface control to reveal such identifying information. For example, a wireless picture frame device typically lacks a control interface read or extract identification information, such as a MAC address.

While some wireless devices include a user interface for dedicated device functionality, e.g. such as a user control for a game box or a digital video recorder, a dedicated user interface is often incapable or cumbersome to be used to communicate device identification and to exchange provisioning information. In addition, while some wireless devices provide a user interface control which can reveal such identifying information, provisioning procedures still require a user to be technically proficient to properly initiate and complete a provisioning process.

It would therefore be advantageous to provide a network provisioning system, which does not require a user interface for the initiation of a provisioning process. The development of such a wireless access provisioning system would constitute a major technological advance.

Furthermore, it would be advantageous to provide a wireless access provisioning structure and process with minimal device requirements and/or user proficiency, whereby a wireless device is readily provisioned by the provisioning system, and whereby other devices within an access region are prevented from being provisioned by the provisioning system. The development of such a provisioning system would constitute a further technological advance.

As well, it would be advantageous that such a wireless access provisioning system be integrated with easily monitored parameters of a wireless device, such as the time monitoring of power on and/or start of signal transmission. The development of such a provisioning system would constitute a further major technological advance. The development of such a time-based wireless access provisioning system for provisioning secure encrypted communication would constitute a further technological advance.

### SUMMARY OF THE INVENTION

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter, such as the power on, of the wireless device

4

occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic plan view of a time based wireless access provisioning system;

FIG. 2 is a functional block diagram of a time based wireless access provisioning system;

FIG. 3 is a flow chart of a time based wireless access provisioning process;

FIG. 4 is a flow chart of an alternate time based wireless access provisioning process;

FIG. 5 shows a simplified timeline for a time based wireless access provisioning process;

FIG. 6 shows a simplified timeline for an alternate time based wireless access provisioning process; and

FIG. 7 shows the time-based acceptance and provisioning of a new wireless device within a time based wireless access provisioning system.

### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 is a schematic plan view 10 of a time based wireless access provisioning system 20. FIG. 2 is a functional block diagram of a time based wireless access provisioning system 20, comprising a network access point 12 adapted to provide time-based provisioning with a wireless device 14.

The network access point 12 shown in FIG. 2 comprises a transceiver 32 and antenna 34, which provides communication 16 to one or more wireless devices 14. The communications channel 16 typically comprises an input, i.e. reverse link, signal 28 from a wireless device 14 to the access point, as well as an output, i.e. forward link, signal 30, from the access point 12 to the wireless device 14.

As seen in FIG. 2, the network access point 12 typically comprises network logic & componentry 36, such as networking functions 40, thereby providing communications between one or more authorized wireless devices 14 and a local network 17 (FIG. 1). The network access point 12 shown in FIG. 1 also comprises a network connection 38 to one or more networks 39, such as to wired devices within a LAN, and/or to other networks, such as the Internet. The network access point 12 shown in FIG. 2 comprises an access control list 42, which identifies wireless devices 14 which have proper access to the local network 17 (FIG. 1), such as by storing accepted device identifications 50 as list elements 43a–43n.

The wireless device 14 shown in FIG. 2 comprises a device transceiver 22 and antenna 24, which provides communication 16 to the network access point 12, and in some embodiments to other wireless devices 14. The wireless device 14 comprises communication logic and componentry 48, and comprises an associated device identifier 50, e.g. such as a unique MAC address, which is communicatable to the network access point 12, whereby the wireless device 14 can be controllably provisioned into the network 17 by the network access point 12. The wireless device 14 also com-

US 7,177,285 B2

5

prises power 26, e.g. wired or battery, and power activation 26. In some embodiments of the time based wireless access provisioning system 20, the wireless device is an IEEE 802.11 WLAN and/or Bluetooth™ compliant device.

The network access point 12 shown in FIG. 1 is located within a service area 18 for a network 17, such as a wireless local area network (WLAN) or a wireless personal area network (WPAN), and typically communicates 16 with a one or more wireless devices 14 which operate within the service area 18, as well as to other wired devices connected to the network, and to connected networks, such as the Internet.

As seen in FIG. 1, the time based wireless access provisioning system 20 can be used for a wide variety of wireless devices 14a–14n which are adapted to communicate with the network access point 12, such as but not limited to a desktop computer 14a, a portable laptop computer 14b, a network printer 14c, a digital video recorder 14d, a game box 14e, a portable phone 14f, a personal digital assistant (PDA) 14g, and/or a wireless picture frame 14h.

The network access point 12 provides time-based provisioning to ensure that only authorized wireless devices 14 can operate within the local network 17, such as within a home HM, and to prevent unauthorized wireless devices 14, such as device 14n in FIG. 1, from gaining access to the network 17.

In the time based wireless access provisioning system 20, the network access point 12 also comprises time based provisioning 44, which is activatable 46, such as manually by a user U. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17. A properly timed interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12 acts to qualify the wireless device 14 to the network access point.

Time-Based Provisioning Process. FIG. 3 is a flow chart of a time based wireless access provisioning process 52a. The network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 5). The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46.

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 3, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, e.g. such as within 5 minutes. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 5), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 3, the time based wireless access provisioning process 52a also prevents network access from devices 14 which are powered on 78 (FIG. 5) at an earlier time 88 (FIG. 5). If a wireless device 14 is powered on at a time 88 before the acceptance time interval 74 (FIG. 5), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device, preventing provisioning 64 into the network 17.

FIG. 5 shows a simplified timeline 70a for a time based wireless access provisioning process 52a. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 5, the network access point 14 notes the start time 82 of the power

6

on 56 of a wireless device 14 which is desired to be provisioned within the network 17. The user then activates provisioning logic 44 at the network access point 12, at time 86. The provisioning logic 44 typically comprises an acceptance time interval 74, e.g. such as a 5 minute interval 74, having a start time 84 and an end time 86, within which desired devices 14 are accepted 62 (FIG. 3). As seen in FIG. 5, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 5, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12. When the user activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, i.e. failing 66 time-based determination 60 (FIG. 3) such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Alternate Time-Based Provisioning Process. FIG. 4 is a flow chart of an alternate time based wireless access provisioning process 52b, in which a desired wireless device 14 to be provisioned is powered on after the provisioning logic 44 is activated. As above, the network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 6).

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 4, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, after the provisioning logic 44 is activated 58. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 6), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 4, the alternate time based wireless access provisioning process 52b also prevents network access from devices 14 which are powered on 78 (FIG. 6) at an earlier time 88 (FIG. 6). If a wireless device 14 is powered on at a time 88 before (or after) the acceptance time interval 74 (FIG. 6), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device 14, preventing provisioning 64 into the network 17.

FIG. 6 shows a simplified timeline 70b for the alternate time based wireless access provisioning process 52b. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 6, the user activates provisioning logic 44 at the network access point 12, at time 84. The network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. If the power on 56 falls within the acceptance time interval 74, the desired device 14 is accepted 62 (FIG. 4). As seen in FIG. 6, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 6, the network access point 14 also notes the start time 88 of the power on 78 of a second



US 7,177,285 B2

7

wireless device 14, which is not necessarily desired to be provisioned by the network access point 12, such as from an unauthorized device 14, or from a desired device which is not powered on within the time interval 74. When the user then activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, and before the activation 58 of the provisioning logic 44, such that the provisioning logic 44 denies 66 the second wireless device 14, and prevents provisioning 64.

Device Qualification. FIG. 7 provides a schematic view 90 of a time-based acceptance of a new wireless device 14 within a time based wireless access provisioning system 20.

When at the provisioning logic 44 time-qualifies 62 (FIG. 3, FIG. 4) a wireless device 14, the wireless access point 12 accepts the time-based qualification 57, and initiates the provisioning process 64, which typically comprises communication 16 and secure provisioning of information between the wireless device 14 and the network access point 12, such as the exchange of key material, if an encryption protocol is to be used. Device parameters, such as the device identifier 50, are typically sent 92 to the access point 12, wherein the device identifier 50 is added to the network access control list 42. As seen in FIG. 7, the device identifier 50 for the accepted wireless device 14 is added to the access control list 42, such as an element 43b in the list of qualified devices 14. Provisioning information may also be sent 94 from the network access point to the device, such as to establish setup, handshaking, or encryption provisioning.

System Implementation. The time-based wireless access provisioning system 20 readily integrates one or more wireless devices 14 into a local area network in a secure fashion. For example, when a user U brings home a new wireless device 14 for use in their existing home network 17, the time-based wireless access provisioning system 20 allows the user U to easily add the new device to the network 17, without exposing the network unnecessarily to attack from third parties.

Within the time based access provisioning system 20, the enhanced network access point 12 keeps track of all wireless devices 14a-14n in the vicinity 18 of the central access point 12. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17, based upon a properly timed device qualification interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12.

As seen in FIG. 3 and FIG. 4, when a user U brings a device 14 home HM and powers on the wireless device 14, the user then simply presses a button 46 on their network access point 12. In response thereto, the access point 12 provisions the wireless device automatically, based on the time-based qualification 57. Since the access point 12 is only available for such provisioning for a short interval 74 after the button 46 is pressed, it is unlikely that the access point 12 will provision unauthorized third party devices 14.

The qualification protocol 52a, 52b allows the network access point 12 to augment the access control list 42 with a properly qualified device 14. The network access point can discount, i.e. deny, devices in neighboring residences HM that have been on for a long time, wherein power on 78 of the devices 14 extends beyond the acceptance interval 74, and can identify and provision one or more devices 14 that are powered on 56 within the acceptance interval 74.

The time-based access provisioning system 20 does not require a user interface on a wireless device 14 to initiate device setup and provisioning. As the power on or beginning

8

of signal transmission 16 is easily tracked by the enhanced network access point 12, a simple activation 46, such as the pushing of a button 46, can be used to time-qualify 57 a desired device 14, and to deny qualification 66 for an unqualified device. Therefore, the time-based access provisioning system 20 drastically simplifies wireless setup and provisioning for wireless devices. Wireless devices 14 to be provisioned are not required to have complex user interfaces, and users are not required to perform complex provisioning procedures. The time-based access provisioning system 20 simplifies the integration of wireless devices into a network, and provides more than reasonable levels of security.

Alternate Applications for the Time-Based Access Provisioning System.

While the time based access provisioning system 10 is disclosed above as tracking a single power on 56, 78 of wireless devices, alternate embodiments of the time based access provisioning system 10 provide further network protections from undesired devices.

For example, for a neighboring device which is switched on and off repeatedly, such as for an undesired wireless device or user in search of a network access point 12, the network access point 12 tracks the repeated powering operation, and can deny provisioning access as desired.

Although the time based access provisioning system and its methods of use are described herein in connection with wireless devices, personal computers and other microprocessor-based devices, such as wireless appliances, the apparatus and techniques can be implemented for a wide variety of electronic devices and systems, or any combination thereof, as desired.

Furthermore, while the time based access provisioning system and its methods of use are described herein in connection with wireless devices and intranets or LAN's, the apparatus and techniques can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

As well, while the time based access provisioning system and its methods of use are described herein in connection with a time based interaction between a wireless device and a network access point, the use of tracking power on/off as a signal to associate devices automatically can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.

What is claimed is:

1. A process for provisioning between a wireless device and a network, comprising the steps of:

tracking an operating parameter of the wireless device within a service area, wherein the operating parameter of the wireless device comprises an onset of a signal transmission of the wireless device; and

initiating provisioning of the wireless device if the tracked operating parameter occurs within a time interval.

2. The process of claim 1, wherein the wireless device comprises any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

## US 7,177,285 B2

9

3. The process of claim 1, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

4. The process of claim 1, wherein the provisioning is prevented if the tracked operating parameter occurs outside the time interval, comprising any of before the time interval and after the time interval.

5. The process of claim 1, wherein the provisioning is prevented if the tracked operating parameter occurs repeatedly.

6. The process of claim 1, wherein the provisioning is performed automatically.

7. The process of claim 1, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

8. The process of claim 1, wherein the provisioning comprises transmitting information to the wireless device, wherein the transmitted information comprises any of setup information, handshaking information, and encryption information.

9. The process of claim 1, wherein the provisioning comprises receiving information from the wireless device.

10. The process of claim 9, wherein the received information comprises a device identifier.

11. The process of claim 10, wherein the device identifier comprises a MAC address.

12. The process of claim 1, further comprising the step of: providing an access point that tracks the operating parameter of the wireless device.

13. The process of claim 12, further comprising the step of: activating the time interval through the access point.

14. The process of claim 12, wherein the access point comprises means for activating the time interval, wherein the activation means comprises any of a button and a switch.

15. The process of claim 13, wherein the access point comprises an access control list.

16. The process of claim 15, wherein the access control list comprises an identification of one or more wireless devices that have access to the network.

17. The process of claim 12, wherein the access point communicates with one or more wired devices.

18. The process of claim 17, wherein the access point is connected to the wired devices through a local area network (LAN).

19. The process of claim 12, wherein the access point communicates with at least one other wireless device that operates within the service area.

20. The process of claim 12, wherein the access point further comprises a network connection to one or more networks.

21. The process of claim 20, wherein the connected network comprises any of a local area network (LAN) and the Internet.

22. A system for provisioning between a wireless device and a network, comprising:

means for tracking an operating parameter of the wireless device within a service area, wherein the tracked operating parameter of the wireless device comprises an onset of a signal transmission of the wireless device; and

logic for initiating provisioning of the wireless device if the tracked operating parameter occurs within a time interval.

23. The system of claim 22, wherein the wireless device comprises any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless

10

picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, and a digital music player.

24. The system of claim 22, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

25. The system of claim 22, wherein the provisioning is prevented if the tracked operating parameter occurs outside the time interval, comprising any of before the time interval and after the time interval.

26. The system of claim 22, wherein the provisioning is prevented if the tracked operating parameter occurs repeatedly.

27. The system of claim 22, wherein the provisioning is performed automatically.

28. The system of claim 22, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

29. The system of claim 22, wherein the provisioning comprises transmitting information to the wireless device, wherein the transmitted information comprises any of setup information, handshaking information, and encryption information.

30. The system of claim 22, wherein the provisioning comprises a reception of information from the wireless device.

31. The system of claim 30, wherein the received information comprises a device identifier.

32. The system of claim 31, wherein the device identifier comprises a MAC address.

33. The system of claim 22, wherein the tracking means comprises an access point.

34. The system of claim 33, further comprising: an activation of the time interval through the access point.

35. The system of claim 33, wherein the access point comprises means for activating the time interval, wherein the activation means comprises any of a button and a switch.

36. The system of claim 33, wherein the access point comprises an access control list.

37. The system of claim 36, wherein the access control list comprises an identification of one or more wireless devices that have access to the network.

38. The system of claim 33, wherein the access point communicates with one or more wired devices.

39. The system of claim 38, wherein the access point is connected to the wired devices through a local area network (LAN).

40. The system of claim 33, wherein the access point communicates with at least one other wireless device that operates within the service area.

41. The system of claim 33, wherein the access point further comprises a network connection to one or more networks.

42. The system of claim 41, wherein the connected network comprises any of a local area network (LAN) and the Internet.

43. An access point, comprising:  
means for tracking an operating parameter of a wireless device, wherein the tracked operating parameter of the wireless device comprises any of a power on, and an onset of a signal transmission of the wireless device; and

logic for initiating an association of the wireless device with a network if the tracked operating parameter occurs within a time interval.

44. The access point of claim 43, wherein the wireless device comprises any of a computer, a portable computer, a

## US 7,177,285 B2

## 11

printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera and a digital music player.

45. The access point of claim 43, wherein the wireless device comprises any of an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

46. The access point of claim 43, wherein the association is prevented if the tracked operating parameter occurs outside the time interval, comprising any of before the time interval and after the time interval.

47. The access point of claim 43, wherein the association is prevented if the tracked operating parameter occurs repeatably.

48. The access point of claim 43, wherein the initiation of the association is automatically performable.

49. The access point of claim 43, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

50. The access point of claim 43, wherein the association comprises a transmission of information to the wireless device, wherein the information comprises any of setup information, handshaking information, and encryption information.

51. The access point of claim 43, wherein the association comprises a reception of information from the wireless device.

52. The system of claim 51, wherein the received information comprises a device identifier.

## 12

53. The system of claim 52, wherein the device identifier comprises a MAC address.

54. The access point of claim 43, wherein the time interval is activatable through the access point.

55. The access point of claim 54, wherein the access point comprises means for activating the time interval, comprising any of a button and a switch.

56. The access point of claim 43, further comprising: an access control list.

57. The access point of claim 56, wherein the access control list comprises an identification of one or more wireless devices that have access to the network.

58. The access point of claim 43, wherein the access point is in communication with one or more wired devices.

59. The access point of claim 58, wherein the access point is connected to the wired devices through a local area network (LAN).

60. The access point of claim 43, wherein the access point is in communication with at least one other wireless device that operates within the region.

61. The access point of claim 43, further comprising: a connection to at least a second network.

62. The system of claim 61, wherein the second network comprises any of a local area network (LAN) and the Internet.

\* \* \* \* \*



# Exhibit H

---



US007463596B2

(12) **United States Patent**  
**Roskind et al.**

(10) **Patent No.:** **US 7,463,596 B2**  
(45) **Date of Patent:** **\*Dec. 9, 2008**

(54) **TIME BASED WIRELESS ACCESS  
PROVISIONING**

6,272,129 B1 8/2001 Dynarski et al.

(75) Inventors: **James A. Roskind**, Redwood City, CA  
(US); **John D. Robinson**, South Riding,  
VA (US)

(Continued)

#### FOREIGN PATENT DOCUMENTS

(73) Assignee: **AOL LLC**, Dulles, VA (US)

EP 0814623 12/1997

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 0 days.

(Continued)

#### OTHER PUBLICATIONS

This patent is subject to a terminal dis-  
claimer.

*Security Issues for Wearable Computing and Bluetooth Technology*;  
Catharina Candolin, undated.

(21) Appl. No.: **11/673,513**

(Continued)

(22) Filed: **Feb. 9, 2007**

*Primary Examiner*—Melvin Marcelo

(65) **Prior Publication Data**

(74) *Attorney, Agent, or Firm*—Michael A. Glenn; Glenn  
Patent Group

US 2007/0135060 A1 Jun. 14, 2007

(57) **ABSTRACT**

#### Related U.S. Application Data

(63) Continuation of application No. 10/961,959, filed on  
Oct. 8, 2004, now Pat. No. 7,177,285, which is a con-  
tinuation of application No. 10/341,847, filed on Jan.  
13, 2003, now Pat. No. 6,891,807.

(51) **Int. Cl.**  
**H04L 12/26** (2006.01)  
**H04Q 7/34** (2006.01)

(52) **U.S. Cl.** ..... **370/255; 370/338**

(58) **Field of Classification Search** ..... **370/255,**  
**370/338**

See application file for complete search history.

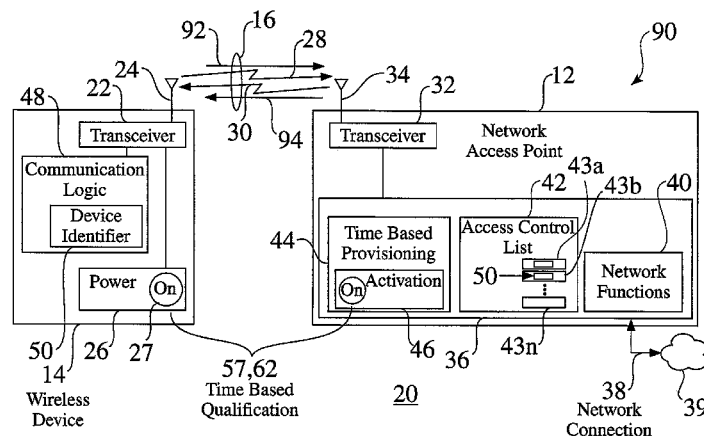
(56) **References Cited**

#### U.S. PATENT DOCUMENTS

5,461,627 A 10/1995 Rypinski  
6,058,106 A 5/2000 Cudak et al.  
6,167,428 A 12/2000 Ellis

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter (such as power on or the onset of signal transmission) of the wireless device occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. In one system embodiment, the network access point tracks the power on time of wireless devices. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

**30 Claims, 7 Drawing Sheets**



## US 7,463,596 B2

Page 2

## U.S. PATENT DOCUMENTS

6,275,693	B1	8/2001	Lin et al.	
6,282,183	B1	8/2001	Harris et al.	
6,317,594	B1	11/2001	Gossman et al.	
6,334,056	B1	12/2001	Holmes et al.	
6,359,880	B1	3/2002	Curry et al.	
6,418,146	B1	7/2002	Miloslavsky	
6,418,324	B1	7/2002	Doviak et al.	
6,891,807	B2	5/2005	Roskind et al.	
7,274,931	B2 *	9/2007	Harris	455/419
2001/0048744	A1	12/2001	Kimura	
2003/0152235	A1	8/2003	Cohen et al.	

## FOREIGN PATENT DOCUMENTS

EP	0999672	5/2000
EP	1081895	3/2001
EP	1126681	8/2001
EP	1191763	3/2002
EP	1225778	7/2002
JP	2001-308866	2/2001
WO	WO 01/22661	3/2001

## OTHER PUBLICATIONS

*Privacy and Authentication for Wireless Local Area Networks*; Ashar Aziz, and Whitfield Diffie; Sun Microsystems, Inc.; Jul. 26, 1993.

*Painting Your Home Blue [Bluetooth/sup <sup>TM</sup>/wireless Technology]*; D. Cypher; Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances; Jan. 15-16, 2002.

*Wireless Home Networks Based on a Hierarchical Bluetooth Scatternet Architecture*; W. Lilakiatsakun, A. Seneviratne; Proceedings Ninth IEEE International Conference on Networks; Oct. 10-12, 2001.

*Bluetooth Wireless Technology in the Home*; R. Shepherd; Electronics & Communication Engineering Journal; Oct. 2001.

*Wireless Gateway for Wireless Home AV Network and Its Implementation*; T. Saito, I. Imoda, Y. Takabatke, and K. Teramoto, and K. Fujimoto; IEEE Transactions on Consumer Electronics; Aug. 2001.

*A Wireless Home Network and Its Application Systems*; H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura; IEEE Transactions on Consumer Electronics; May 2000.

*Wireless Home Link*; IEICE Transactions on Communications; Dec. 1999.

*An Access Protocol for a Wireless Home Network*; A.C.V. Gummalia, and J.O. Limb; WCNC. 1999 IEEE Wireless Communications and Networking Conference; Sep. 21-24, 1999.

*Firewalls for Security in Wireless Networks*; U. Murthy, O. Bukhres, W. Winn, and E. Vanderdez; Proceedings of the Thirty-First Hawaii International Conference on System sciences; Jan. 6-9, 1998.

*Self-Securing Ad Hoc Wireless Networks*; Haiyun Luo, Petros Aferos, Jiejun Kng, Songwu Lu, and Lixia Zhang, undated.

*Wireless Networking for Control and Automation of Off-Road Equipment*; by J.D. Will; An ASAE Meeting Presentation, undated.

*Intrusion Detection in Wireless Ad-Hoc Networks*; Yongguang Zhang and Wenke Lee; Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking; Aug. 6-11, 2000.

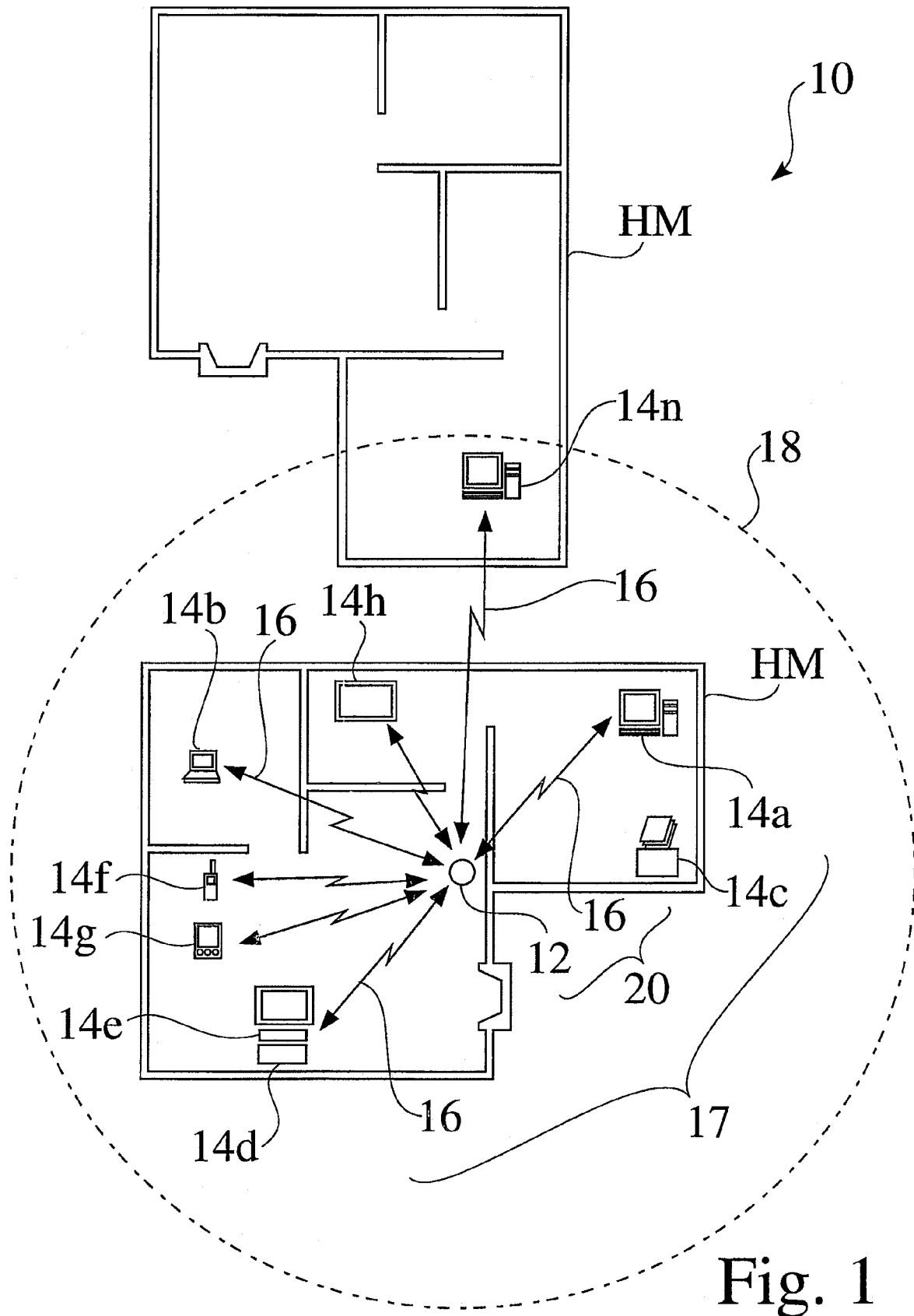
*Microsoft Announces Wireless Provisioning Services*; GeekZone; Wi-Fi, posted Dec. 10, 2003 20:56:21 NZ.

*HP Spotlights Mobile Gear*; Ina Fried; CNET News.com; Oct. 13, 2003.

*Wireless Provisioning Services Overview*; The Cable Guy—Dec. 2003; TechNet Newsletter; 2004 Microsoft Corporation.

Sony Ericsson Mobile Communications; *Sony Ericsson HBH-65* (Manual); Pub #LZT 1086746 R1A; 1<sup>st</sup> Ed. Aug. 2003; Sony Ericsson Mobile Communications, AB.

\* cited by examiner



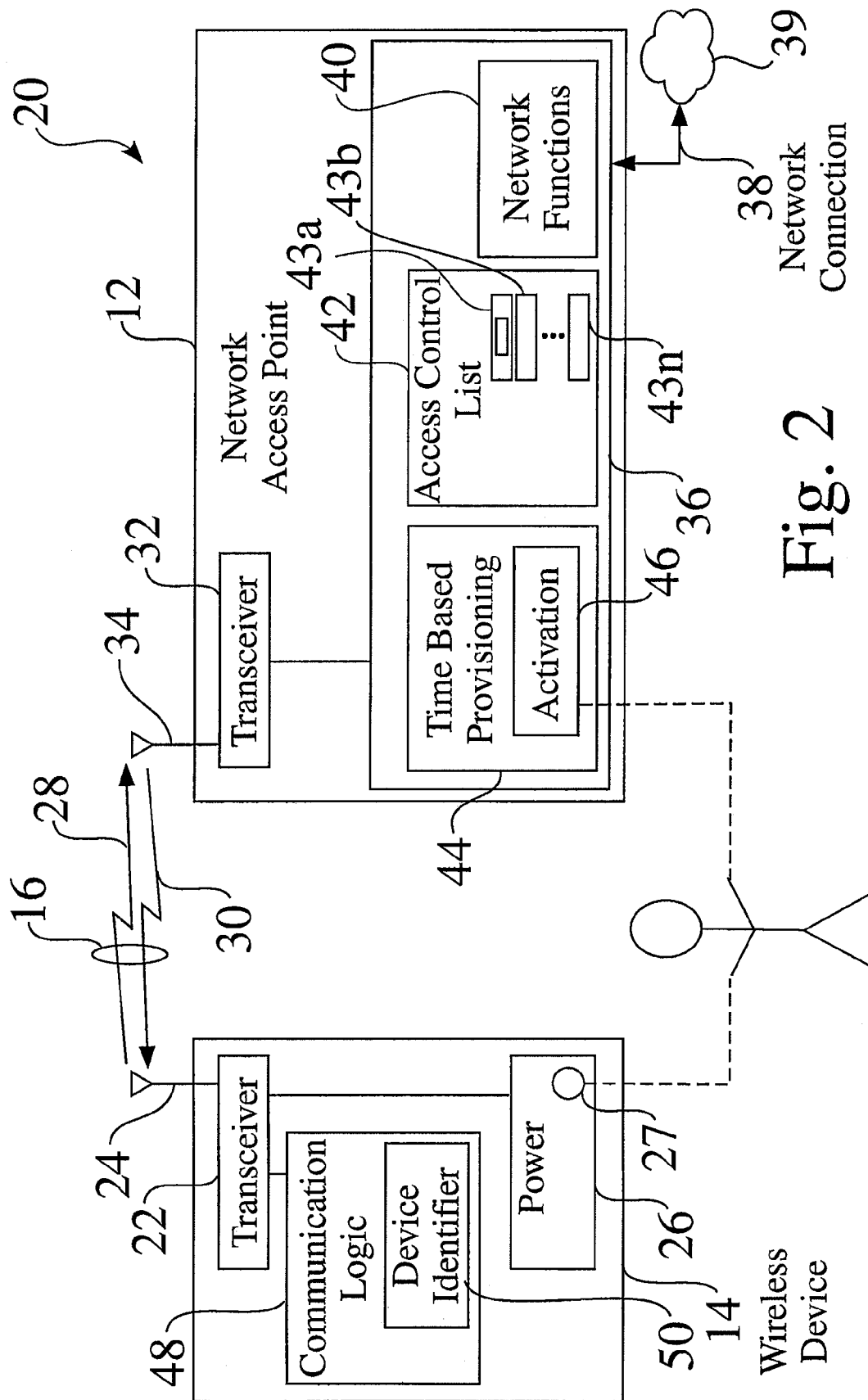


Fig. 2

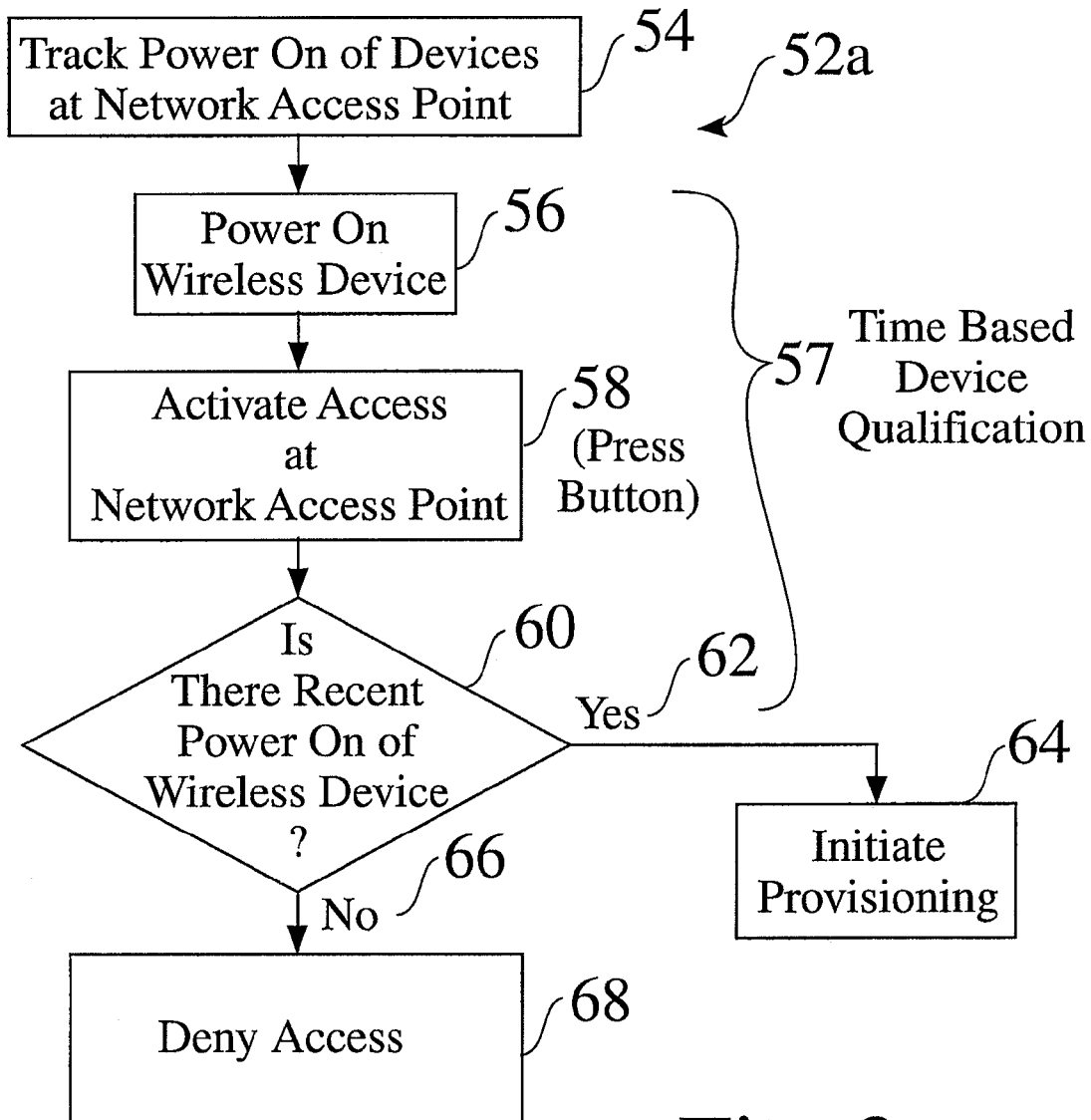


Fig. 3



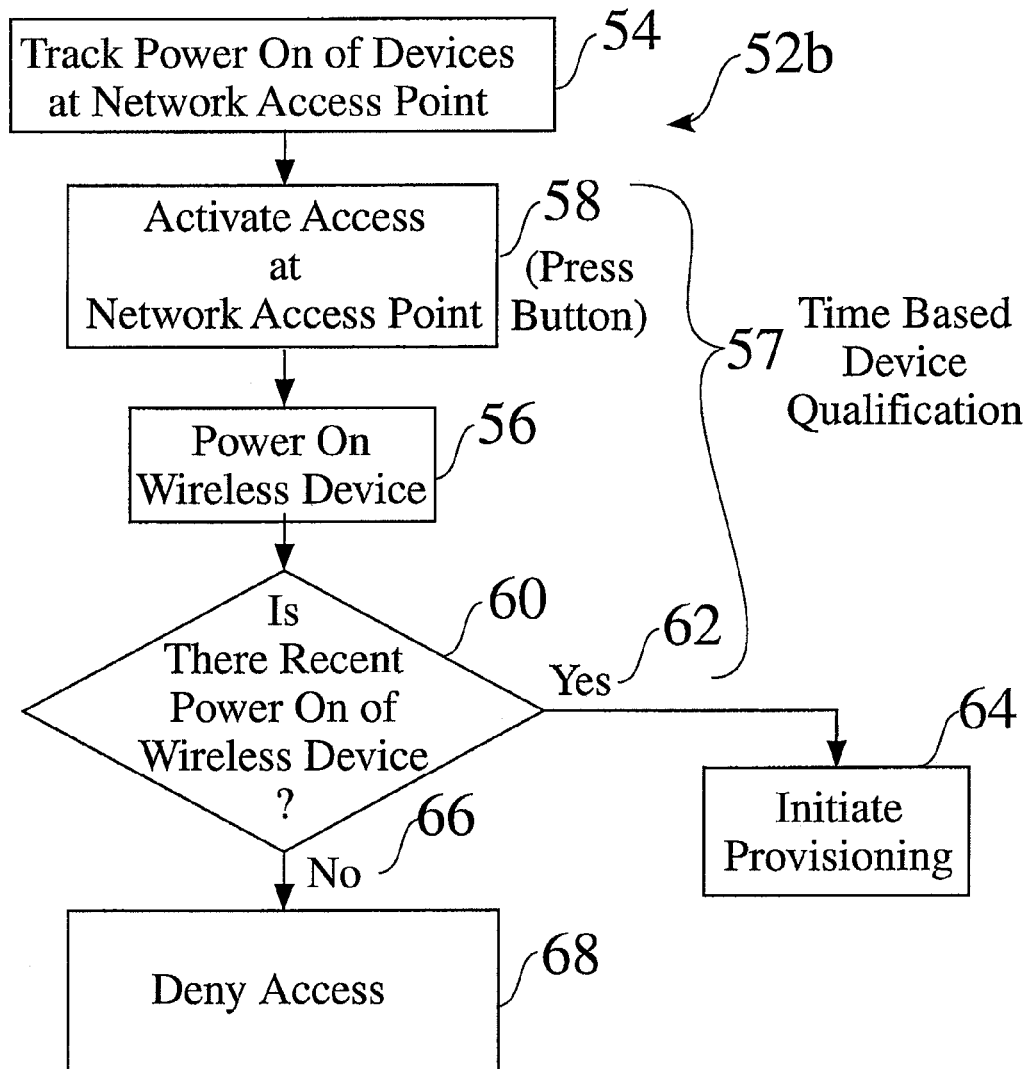


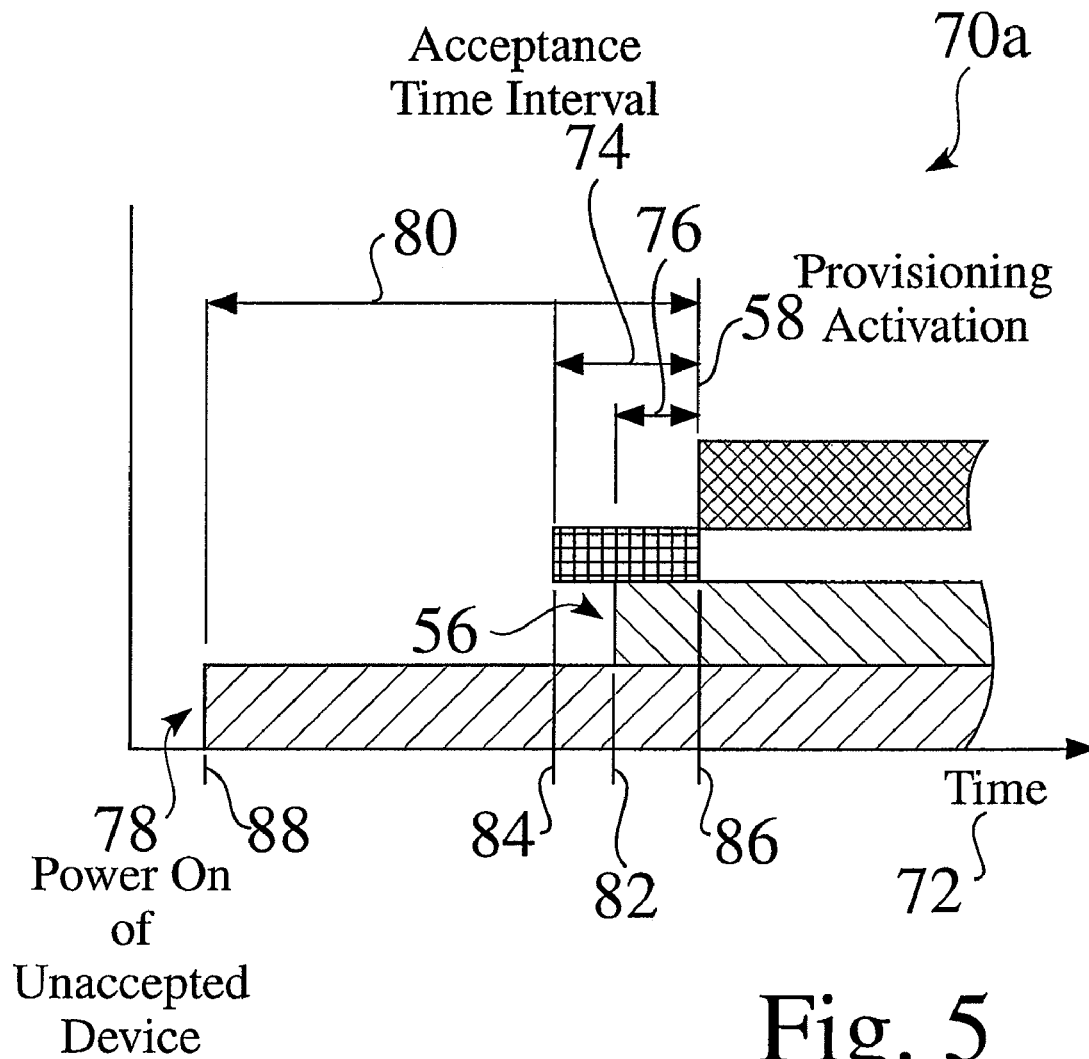
Fig. 4

U.S. Patent

Dec. 9, 2008

Sheet 5 of 7

US 7,463,596 B2



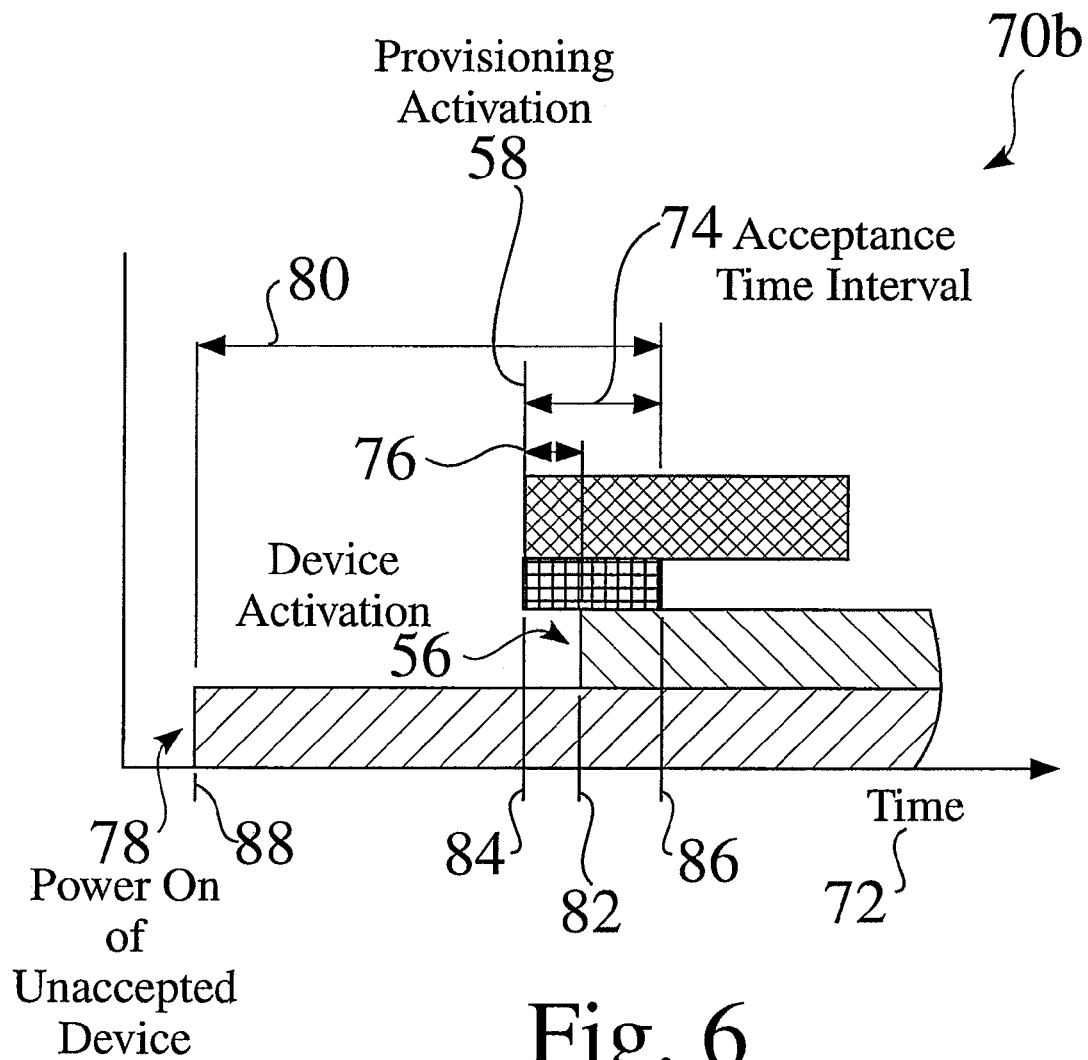
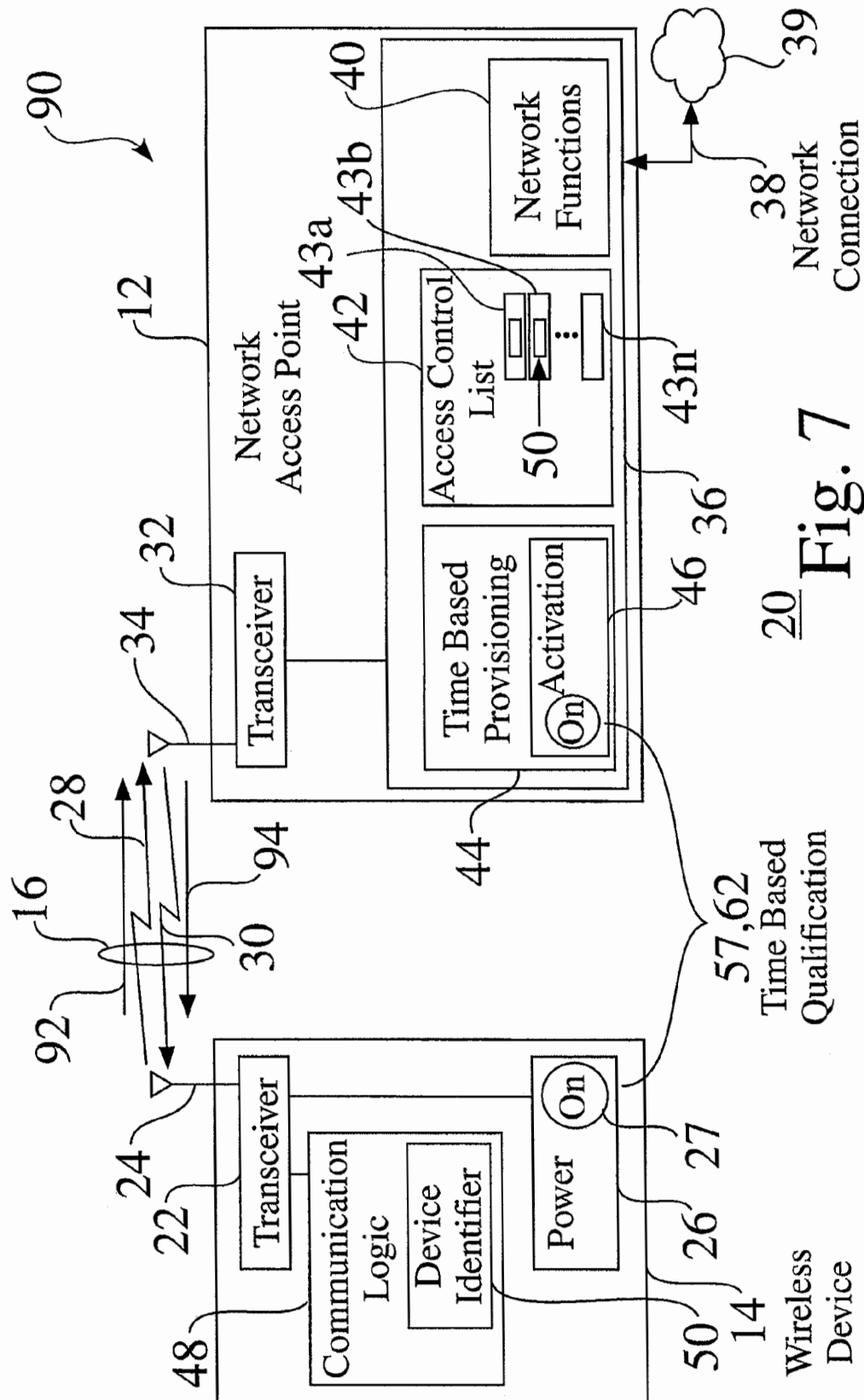


Fig. 6



US 7,463,596 B2

1

**TIME BASED WIRELESS ACCESS  
PROVISIONING****CROSS REFERENCE TO RELATED  
APPLICATIONS**

This application is a Continuation of U.S. Ser. No. 10/961, 959, filed Oct. 8, 2004 now U.S. Pat. No. 7,177,285, which is a Continuation of U.S. Ser. No. 10/341,847, filed Jan. 13, 2003, which was issued as U.S. Pat. No. 6,891,807 on May 10, 2005, each of which are incorporated herein in their entirety by this reference thereto.

**FIELD OF THE INVENTION**

The invention relates to the field of wireless connections between a wireless device and a network. More particularly, the invention relates to access provisioning between one or more wireless devices and an intranet access point.

**BACKGROUND OF THE INVENTION**

In local area networks, such as wireless home networks, one or more wireless devices, e.g. such as IEEE 802.11b devices, are linked to the network by a provisioning process through a network access point. When a user acquires a new wireless device, they need to securely tie it to their intranet, which comprises telling the intranet to accept wireless communications from the device, as well as provisioning the device with key material, such as for creating an encrypted connection. In conventional networks having one or more devices to be provisioned to a network access point, device identification information, such as a MAC address, is required to be communicated from the wireless device to the access point.

Several methods have been described for wireless access provisioning to integrate wireless devices into a network.

M. Cudak, B. Mueller, J. Kelton, and B. Classon, Network Protocol Method, Access Point Device and Peripheral Devices for Providing for an Efficient Centrally Coordinated Peer-to-Peer Wireless Communications Network, U.S. Pat. No. 6,058,106, discloses a "peer-to-peer wireless communications network wherein the access point device: (1) broadcasts a block assignment that specifies a wireless source peripheral device and a wireless destination peripheral device; (2) receives, from the wireless destination peripheral device, sequence information; (3) determines whether the sequence information represents one of: a negative acknowledgment and a positive acknowledgment with a sequence number; (4) forwards an acknowledgment to the wireless source peripheral based on the sequence information, and repeats steps (1)-(4) until N blocks of data, N a predetermined integer, have been transferred from the wireless source peripheral to the wireless destination peripheral."

J. Lin, P. Alfano, and S. Upp, Method and Apparatus for Performing Bearer Independent Wireless Application Service Provisioning, U.S. Pat. No. 6,275,693 disclose a provisioning system, in which a "mobile communication device contacts a provisioning proxy over the wireless bearer network, which in turns contacts a provisioning center over a public network. A provisioning tunnel is then established between the provisioning center and the mobile communication device. Once the provisioning tunnel is set up, the user of the mobile communication device can subscribe to, or unsubscribe from wireless application services."

Wireless Device Registering Method in Wireless Home Network, PCT Patent Application No. WO 01/2266,

2

describes the sending of an authentication key to a device for storage, when an identification code received from the device corresponds to a code stored in an access point.

Secure Wireless LAN, European Pat. No. EP, 1081895, discloses wireless device use by a wireless device operator with an access point connected to a wired LAN in communication with the wireless device through air channel authentication.

C. Candolin, *Security Issues for Wearable Computing and Bluetooth Technology*, 23 Oct. 2000, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, P.B. 400, FIN-02015 HUT, Finland, describes Bluetooth Technology as "a short-range wireless cable replacement technology enabling restricted types of ad hoc networks to be formed. All the while, a need for connecting wearable devices, such as PDAs, mobile phones, and mp3-players, is rising. Such networks may be formed using Bluetooth technology, but issues such as security must be taken into consideration. Although an attempt to tackle security is made, the result is too weak to be used for anything else than for personal purposes."

Other systems provide various details of the operation of wireless devices within a network, such as U.S. Pat. No. 6,418,324, Apparatus and Method for Transparent Wireless Communication; U.S. Pat. No. 6,418,146, Integrated Communication Center Functionality for WAP Devices; U.S. Pat. No. 6,359,880, Public Wireless/Cordless Internet Gateway; U.S. Pat. No. 6,334,056, Secure Gateway Processing for Handheld Device Markup Language; U.S. Pat. No. 6,317,594, System and Method for Providing Data to a Wireless Device Upon Detection of Activity of the Device on a Wireless Network; U.S. Pat. No. 6,282,183, Method for Authorizing Coupling between devices in a Capability Addressable Network; U.S. Pat. No. 6,272,129, Dynamic Allocation of Wireless Mobile Nodes Over An Internet Protocol (IP) Network; U.S. Pat. No. 6,167,428, Personal Computer Microprocessor Firewalls for Internet Distributed Processing; European Pat. No. 1225778, Wireless Repeater Using Identification of Call Originator, European Pat. No. EP 1191763, Access Authentication System for a Wireless Environment; European Pat. No. 1126681, A Network Portal System and Methods; European Pat. No. EP1081895, Secure Wireless Local Area Network; European Pat. No. EP 999672, System and Method for Mapping Packet Data Functional Entities to Elements in a Communications Network; European Pat. No. EP814623, Mobile Decision Methodology for Accessing Multiple Wireless Data Networks; *Privacy and Authentication for Wireless Local Area Networks*, Ashar Aziz and Whitfield Diffie; Sun Microsystems, Inc., Jul. 26, 1993; *Painting Your Home Blue (Bluetooth™ Wireless Technology)*, D. Cypher, Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances, Jan. 15-16, 2002; *Wireless Home Networks on a Hierarchical Bluetooth Scatternet Architecture*, W. Lilakiatsakun, A. Seneviratne, Proceedings Ninth IEEE International Conference on Networks; Oct. 10-12, 2001; *Bluetooth Wireless Technology in the Home*, R. Shephard, Electronics & Communication Engineering Journal; October 2001; *Wireless Gateway for Wireless Home AV Network and Its Implementation*, T. Saito, I. Imoda, Y. Takabake, K. Teramoto, and K. Fujimoto, IEEE Transactions on Consumer Electronics, August 2001; *A Wireless Home Network and its Applications Systems*, H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura, IEEE Transactions on Consumer Electronics, May 2000; *Wireless Home Link*, M. Nakagawa, IEICE Transactions on Communications, December 1999; *An Access Protocol for a Wireless Home Network*, A. C. V. Gummalla, and J. O. Limb, WCNC 1999 IEEE Wireless

US 7,463,596 B2

3

Communications and Networking Conference; Sep. 21-24, 1999; *Firewalls for Security in Wireless Networks*, U. Murthy, O. Bukres, W. Winn, and E. Vanderdez, Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Jan. 6-9, 1998; *Self-Securing Ad Hoc Wireless Networks*, Haiyun Luo, Petros Aerfos, Jiejun Kng, Songwu Lu, and Lixia Zhang; *Wireless Networking for Control and Automation of Off-Road Equipment*, J. D. Will; ASAE Meeting Presentation; and *Intrusion Detection in Wireless Ad-Hoc Networks*, Yongguang Zhang and Wenke Lee, Proceeding of the Sixth Annual International Conference on Mobile Computing and Networking, Aug. 6-11, 2000.

The disclosed prior art systems and methodologies thus provide basic provisioning for wireless devices to a network through an access point. However, for many networks, such provisioning schemes are often impractical, either for wireless devices which lack a user interface which is configured for communicating provisioning information, or for simple home-based intranets. For example, device identification information, such as a MAC address, is often required to be manually transcribed from the wireless device to the access point, since wireless devices often lack a user interface control to reveal such identifying information. For example, a wireless picture frame device typically lacks a control interface read or extract identification information, such as a MAC address.

While some wireless devices include a user interface for dedicated device functionality, e.g. such as a user control for a game box or a digital video recorder, a dedicated user interface is often incapable or cumbersome to be used to communicate device identification and to exchange provisioning information. In addition, while some wireless devices provide a user interface control which can reveal such identifying information, provisioning procedures still require a user to be technically proficient to properly initiate and complete a provisioning process.

It would therefore be advantageous to provide a network provisioning system, which does not require a user interface for the initiation of a provisioning process. The development of such a wireless access provisioning system would constitute a major technological advance.

Furthermore, it would be advantageous to provide a wireless access provisioning structure and process with minimal device requirements and/or user proficiency, whereby a wireless device is readily provisioned by the provisioning system, and whereby other devices within an access region are prevented from being provisioned by the provisioning system. The development of such a provisioning system would constitute a further technological advance.

As well, it would be advantageous that such a wireless access provisioning system be integrated with easily monitored parameters of a wireless device, such as the time monitoring of power on and/or start of signal transmission. The development of such a provisioning system would constitute a further major technological advance. The development of such a time-based wireless access provisioning system for provisioning secure encrypted communication would constitute a further technological advance.

### SUMMARY OF THE INVENTION

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter, such as the power on, of the wireless device occurs

4

within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic plan view of a time based wireless access provisioning system;

FIG. 2 is a functional block diagram of a time based wireless access provisioning system;

FIG. 3 is a flow chart of a time based wireless access provisioning process;

FIG. 4 is a flow chart of an alternate time based wireless access provisioning process;

FIG. 5 shows a simplified timeline for a time based wireless access provisioning process;

FIG. 6 shows a simplified timeline for an alternate time based wireless access provisioning process; and

FIG. 7 shows the time-based acceptance and provisioning of a new wireless device within a time based wireless access provisioning system.

### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 is a schematic plan view of a time based wireless access provisioning system. FIG. 2 is a functional block diagram of a time based wireless access provisioning system, comprising a network access point 12 adapted to provide time-based provisioning with a wireless device 14.

The network access point 12 shown in FIG. 2 comprises a transceiver 32 and antenna 34, which provides communication 16 to one or more wireless devices 14. The communication channel 16 typically comprises an input, i.e. reverse link, signal 28 from a wireless device 14 to the access point, as well as an output, i.e. forward link, signal 30, from the access point 12 to the wireless device 14.

As seen in FIG. 2, the network access point 12 typically comprises network logic & componentry 36, such as networking functions 40, thereby providing communications between one or more authorized wireless devices 14 and a local network 17 (FIG. 1). The network access point 12 shown in FIG. 1 also comprises a network connection 38 to one or more networks 39, such as to wired devices within a LAN, and/or to other networks, such as the Internet. The network access point 12 shown in FIG. 2 comprises an access control list 42, which identifies wireless devices 14 which have proper access to the local network 17 (FIG. 1), such as by storing accepted device identifications 50 as list elements 43a-43n.

The wireless device 14 shown in FIG. 2 comprises a device transceiver 22 and antenna 24, which provides communication 16 to the network access point 12, and in some embodiments to other wireless devices 14. The wireless device 14 comprises communication logic and componentry 48, and comprises an associated device identifier 50, e.g. such as a unique MAC address, which is communicatable to the network access point 12, whereby the wireless device 14 can be controllably provisioned into the network 17 by the network access point 12. The wireless device 14 also comprises power 26, e.g. wired or battery, and power activation 26. In some embodiments of the time based wireless access provisioning



US 7,463,596 B2

5

system 20, the wireless device is an IEEE 802.11 WLAN and/or Bluetooth™ compliant device.

The network access point 12 shown in FIG. 1 is located within a service area 18 for a network 17, such as a wireless local area network (WLAN) or a wireless personal area network (WPAN), and typically communicates 16 with a one or more wireless devices 14 which operate within the service area 18, as well as to other wired devices connected to the network, and to connected networks, such as the Internet.

As seen in FIG. 1, the time based wireless access provisioning system 20 can be used for a wide variety of wireless devices 14a-14n which are adapted to communicate with the network access point 12, such as but not limited to a desktop computer 14a, a portable laptop computer 14b, a network printer 14c, a digital video recorder 14d, a game box 14e, a portable phone 14f, a personal digital assistant (PDA) 14g, and/or a wireless picture frame 14h.

The network access point 12 provides time-based provisioning to ensure that only authorized wireless devices 14 can operate within the local network 17, such as within a home HM, and to prevent unauthorized wireless devices 14, such as device 14n in FIG. 1, from gaining access to the network 17.

In the time based wireless access provisioning system 20, the network access point 12 also comprises time based provisioning 44, which is activatable 46, such as manually by a user U. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17. A properly timed interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12 acts to qualify the wireless device 14 to the network access point.

Time-Based Provisioning Process. FIG. 3 is a flow chart of a time based wireless access provisioning process 52a. The network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 5). The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46.

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 3, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, e.g. such as within 5 minutes. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 5), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 3, the time based wireless access provisioning process 52a also prevents network access from devices 14 which are powered on 78 (FIG. 5) at an earlier time 88 (FIG. 5). If a wireless device 14 is powered on at a time 88 before the acceptance time interval 74 (FIG. 5), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device, preventing provisioning 64 into the network 17.

FIG. 5 shows a simplified timeline 70a for a time based wireless access provisioning process 52a. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 5, the network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. The user then activates provisioning logic 44 at the network access point 12, at time 86. The provisioning logic 44 typically comprises an acceptance time interval 74, e.g. such as a 5 minute interval 74, having a start time 84 and

6

an end time 86, within which desired devices 14 are accepted 62 (FIG. 3). As seen in FIG. 5, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 5, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12. When the user activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, i.e. failing 66, time-based determination 60 (FIG. 3) such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Alternate Time-Based Provisioning Process. FIG. 4 is a flow chart of an alternate time based wireless access provisioning process 52b, in which a desired wireless device 14 to be provisioned is powered on after the provisioning logic 44 is activated. As above, the network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 6).

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 4, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, after the provisioning logic 44 is activated 58. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 6), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 4, the alternate time based wireless access provisioning process 52b also prevents network access from devices 14 which are powered on 78 (FIG. 6) at an earlier time 88 (FIG. 6). If a wireless device 14 is powered on at a time 88 before (or after) the acceptance time interval 74 (FIG. 6), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device 14, preventing provisioning 64 into the network 17.

FIG. 6 shows a simplified timeline 70b for the alternate time based wireless access provisioning process 52b. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 6, the user activates provisioning logic 44 at the network access point 12, at time 84. The network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. If the power on 56 falls within the acceptance time interval 74, the desired device 14 is accepted 62 (FIG. 4). As seen in FIG. 6, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 6, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12, such as from an unauthorized device 14, or from a desired device which is not powered on within the time interval 74. When the user then activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside

## US 7,463,596 B2

7

the acceptance interval 74, and before the activation 58 of the provisioning logic 44, such that the provisioning logic 44 denies 66 the second wireless device 14, and prevents provisioning 64.

Device Qualification. FIG. 7 provides a schematic view 90 of a time-based acceptance of a new wireless device 14 within a time based wireless access provisioning system 20.

When a the provisioning logic 44 time-qualifies 62 (FIG. 3, FIG. 4) a wireless device 14, the wireless access point 12 accepts the time-based qualification 57, and initiates the provisioning process 64, which typically comprises communication 16 and secure provisioning of information between the wireless device 14 and the network access point 12, such as the exchange of key material, if an encryption protocol is to be used. Device parameters, such as the device identifier 50, are typically sent 92 to the access point 12, wherein the device identifier 50 is added to the network access control list 42. As seen in FIG. 7, the device identifier 50 for the accepted wireless device 14 is added to the access control list 42, such as an element 43b in the list of qualified devices 14. Provisioning information may also be sent 94 from the network access point to the device, such as to establish setup, handshaking, or encryption provisioning.

System Implementation. The time-based wireless access provisioning system 20 readily integrates one or more wireless devices 14 into a local area network in a secure fashion. For example, when a user U brings home a new wireless device 14 for use in their existing home network 17, the time-based wireless access provisioning system 20 allows the user U to easily add the new device to the network 17, without exposing the network unnecessarily to attack from third parties.

Within the time based access provisioning system 20, the enhanced network access point 12 keeps track of all wireless devices 14a-14n in the vicinity 18 of the central access point 12. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17, based upon a properly timed device qualification interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12.

As seen in FIG. 3 and FIG. 4, when a user U brings a device 14 home HM and powers on the wireless device 14, the user then simply presses a button 46 on their network access point 12. In response thereto, the access point 12 provisions the wireless device automatically, based on the time-based qualification 57. Since the access point 12 is only available for such provisioning for a short interval 74 after the button 46 is pressed, it is unlikely that the access point 12 will provision unauthorized third party devices 14.

The qualification protocol 52a,52b allows the network access point 12 to augment the access control list 42 with a properly qualified device 14. The network access point can discount, i.e. deny, devices in neighboring residences HM that have been on for a long time, wherein power on 78 of the devices 14 extends beyond the acceptance interval 74, and can identify and provision one or more devices 14 that are powered on 56 within the acceptance interval 74.

The time-based access provisioning system 20 does not require a user interface on a wireless device 14 to initiate device setup and provisioning. As the power on or beginning of signal transmission 16 is easily tracked by the enhanced network access point 12, a simple activation 46, such as the pushing of a button 46, can be used to time-qualify 57 a desired device 14, and to deny qualification 66 for an unqualified device. Therefore, the time-based access provisioning system 20 drastically simplifies wireless setup and provision-

8

ing for wireless devices. Wireless devices 14 to be provisioned are not required to have complex user interfaces, and users are not required to perform complex provisioning procedures. The time-based access provisioning system 20 simplifies the integration of wireless devices into a network, and provides more than reasonable levels of security.

Alternate Applications for the Time-Based Access Provisioning System.

While the time based access provisioning system 10 is disclosed above as tracking a single power on 56, 78 of wireless devices, alternate embodiments of the time based access provisioning system 10 provide further network protections from undesired devices.

For example, for a neighboring device which is switched on and off repeatedly, such as for an undesired wireless device or user in search of a network access point 12, the network access point 12 tracks the repeated powering operation, and can deny provisioning access as desired.

Although the time based access provisioning system and its methods of use are described herein in connection with wireless devices, personal computers and other microprocessor-based devices, such as wireless appliances, the apparatus and techniques can be implemented for a wide variety of electronic devices and systems, or any combination thereof, as desired.

Furthermore, while the time based access provisioning system and its methods of use are described herein in connection with wireless devices and intranets or LAN's, the apparatus and techniques can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

As well, while the time based access provisioning system and its methods of use are described herein in connection with a time based interaction between a wireless device and a network access point, the use of tracking power on/off as a signal to associate devices automatically can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.

The invention claimed is:

1. A process for associating devices, comprising the steps of:

tracking an operating parameter of a first device, wherein the operating parameter of the first device comprises any of a power on of the first device, and an onset of a signal transmission of the first device; and

automatically associating the first device with at least one other device if the tracked operating parameter occurs within a time interval.

2. The process of claim 1, wherein any of the first device and at least one of the other devices comprises a wireless device.

3. The process of claim 1, wherein the first device comprises any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, a digital music player, an IEEE 802.11 compliant device and a BLUETOOTH™ compliant device.

4. The process of claim 1, wherein the association is prevented if any of the tracked operating parameter occurs

US 7,463,596 B2

9

repeatedly, and the tracked operating parameter occurs outside the time interval, comprising any of before the time interval and after the time interval.

5. The process of claim 1, wherein any of the first device and at least one of the other devices are located on a network.

6. The process of claim 5, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

7. The process of claim 1, wherein the association comprises any of receiving information from the first device and transmitting information to the first device, wherein the transmitted information comprises any of setup information, handshaking information, and encryption information.

8. The process of claim 7, wherein the received information comprises a device identifier.

9. The process of claim 8, wherein the device identifier comprises a MAC address.

10. The process of claim 1, further comprising the step of: providing an access point that tracks the operating parameter of the first device.

11. The process of claim 10, further comprising the step of: activating the time interval through the access point.

12. The process of claim 10, wherein the access point comprises means for activating the time interval, wherein the activation means comprises any of a button and a switch.

13. The process of claim 10, wherein the access point comprises an identification of one or more devices that have access to a network.

14. The process of claim 10, wherein the access point communicates with one or more wired devices through a network.

15. The process of claim 10, wherein the access point further comprises any of a network connection to one or more networks, and means for communication with at least one other device that operates within a service area.

16. A system for associating devices, comprising:  
means for tracking an operating parameter of a first device, wherein the operating parameter of the first device comprises any of a power on of the first device, and an onset of a signal transmission of the first device; and  
means for automatically associating the first device with at least one other device if the tracked operating parameter occurs within a time interval.

17. The system of claim 16, wherein any of the first device and at least one of the other devices comprises a wireless device.

10

18. The system of claim 16, wherein the first device comprises any of a computer, a portable computer, a printer, a portable phone, a personal digital assistant, a wireless picture frame, a video recording device, an electronic game device, a television, a digital camera, a digital video camera, a digital music player, an IEEE 802.11 compliant device and a BLUE-TOOTH™ compliant device.

19. The system of claim 16, wherein the association is prevented if any of the tracked operating parameter occurs repeatedly, and the tracked operating parameter occurs outside the time interval, comprising any of before the time interval and after the time interval.

20. The system of claim 16, wherein any of the first device and at least one of the other devices are located on a network.

21. The system of claim 20, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

22. The system of claim 16, wherein the association comprises any of a reception of information from the first device and transmission of information to the first device, wherein the transmitted information comprises any of setup information, handshaking information, and encryption information.

23. The system of claim 22, wherein the received information comprises a device identifier.

24. The system of claim 23, wherein the device identifier comprises a MAC address.

25. The system of claim 16, wherein the tracking means comprises an access point.

26. The system of claim 25, further comprising:  
means for activating the time interval through the access point.

27. The system of claim 26, wherein the activation means comprises any of a button and a switch.

28. The system of claim 25, wherein the access point comprises an identification of one or more devices that have access to a network.

29. The system of claim 25, wherein the access point communicates with one or more wired devices through a network.

30. The system of claim 25, wherein the access point further comprises any of a network connection to one or more networks, and means for communication with at least one other device that operates within a service area.

\* \* \* \* \*

# Exhibit I

---



US007911979B2

(12) **United States Patent**  
**Roskind et al.**

(10) **Patent No.:** **US 7,911,979 B2**  
(45) **Date of Patent:** **\*Mar. 22, 2011**

(54) **TIME BASED ACCESS PROVISIONING  
SYSTEM AND PROCESS**

(75) Inventors: **James A. Roskind**, Redwood City, CA  
(US); **John D. Robinson**, South Riding,  
VA (US)

6,167,428 A 12/2000 Ellis  
6,272,129 B1 8/2001 Dynarski et al.  
6,275,693 B1 8/2001 Lin et al.  
6,282,183 B1 8/2001 Harris et al.  
6,317,594 B1 11/2001 Gossman et al.  
6,334,056 B1 12/2001 Holmes et al.

(Continued)

(73) Assignee: **Tarquin Consulting Co., LLC**, Dover,  
DE (US)

**FOREIGN PATENT DOCUMENTS**

EP 0814623 A2 12/1997

(Continued)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 58 days.

This patent is subject to a terminal dis-  
claimer.

**OTHER PUBLICATIONS**

Candolin, Catharina; "Security Issues for Wearable Computing and  
Bluetooth Technology:", undated.

(Continued)

(21) Appl. No.: **12/323,399**

(22) Filed: **Nov. 25, 2008**

*Primary Examiner* — Melvin Marcelo

(65) **Prior Publication Data**

US 2009/0168667 A1 Jul. 2, 2009

(74) *Attorney, Agent, or Firm* — Schwabe, Williamson &  
Wyatt, P.C.

**Related U.S. Application Data**

(63) Continuation of application No. 11/673,513, filed on  
Feb. 9, 2007, now Pat. No. 7,463,596, which is a  
continuation of application No. 10/961,959, filed on  
Oct. 8, 2004, now Pat. No. 7,177,285, which is a  
continuation of application No. 10/341,847, filed on  
Jan. 13, 2003, now Pat. No. 6,891,807.

(51) **Int. Cl.**  
**H04L 12/26** (2006.01)

(52) **U.S. Cl.** ..... **370/255; 370/338**

(58) **Field of Classification Search** ..... **370/255,**  
**370/338**

See application file for complete search history.

(56) **References Cited**

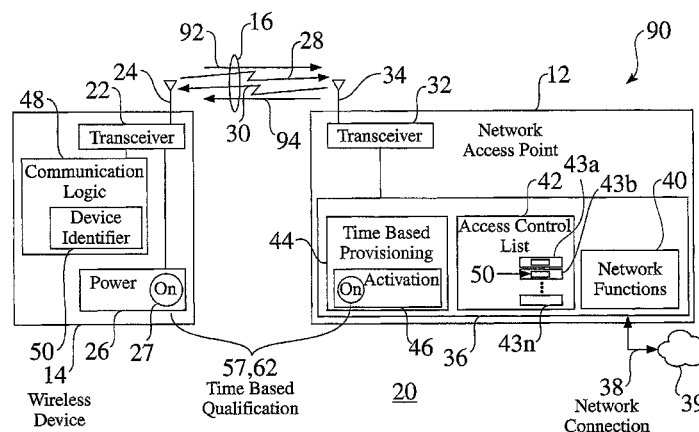
**U.S. PATENT DOCUMENTS**

5,461,627 A 10/1995 Rypinski  
6,058,106 A 5/2000 Cudak et al.

(57) **ABSTRACT**

A method and apparatus is provided for the time-based pro-  
visioning of wireless devices. A network access point moni-  
tors operation of wireless devices within a service region.  
When provisioning logic is activated at the network access  
point, the access point determines if the tracked parameter  
(such as power on or the onset of signal transmission) of the  
wireless device occurs within a designated time interval from  
the time of the provisioning activation. If the tracked device  
qualifies, the network access point proceeds with provision-  
ing the device. In one system embodiment, the network  
access point tracks the power on time of wireless devices.  
When a wireless device to be authorized is powered on, the  
provisioning logic at the network access point notes the  
power on time. The user then activates the provisioning  
access at the network access point, and the network access  
point provisions the wireless device if it is recently powered  
on.

**32 Claims, 7 Drawing Sheets**



**US 7,911,979 B2**

Page 2

**U.S. PATENT DOCUMENTS**

6,359,880	B1	3/2002	Curry et al.
6,418,146	B1	7/2002	Miloslavsky
6,418,324	B1	7/2002	Doviak et al.
6,891,807	B2	5/2005	Roskind et al.
7,274,931	B2	9/2007	Harris
2001/0048744	A1	12/2001	Kimura
2003/0152235	A1	8/2003	Cohen et al.

**FOREIGN PATENT DOCUMENTS**

EP	0999672	A2	5/2000
EP	1081895		3/2001
EP	1126681	A2	8/2001
EP	1191763	A2	3/2002
EP	1225778	A2	7/2002
JP	2001308866		11/2001
WO	WO 0122661		3/2001

**OTHER PUBLICATIONS**

Aziz, et al.; "Privacy and Authentication for Wireless Local Area Networks;" Sun Microsystems, Inc.; Jul. 26, 1993.

Cypher, D.; "Painting your Home Blue [Bluetooth/sup TM/wireless Technology];" Proceedings 2002 IEEE 4.sup.th International Workshop on Networked Appliances; Jan. 15-16, 2002.

Lilakiatsakun, W. et al.; "Wireless Home Networks Based on a Hierarchical Bluetooth Scatternet Architecture;" Proceedings Ninth IEEE International Conference on Networks; Oct. 10-12, 2001.

Shepherd, R.; "Bluetooth Wireless Technology in the Home;" Electronics & Communication Engineering Journal; Oct. 2001.

Saito, T. et al.; "Wireless Gateway for Wireless Home AV Network and Its Implementation"; IEEE Transactions; on consumer Electronics; Aug. 2001.

Fujieda, H. et al.; "A Wireless Home Network and Its Application Systems;" IEEE Transactions on Consumer Electronics; May 2000.

Nakagawa, M.; "Wireless Home Link"; IEICE Transactions on Communications; Dec. 1999.

Gumalla, et al.; "An Access Protocol for a Wireless Home Network;" WCNC. 1999 IEEE Wireless Communications and Networking Conference; Sep. 21-24, 1999, cited by other.

Murthy, U. et al.; "Firewalls for Security in Wireless Networks;" Proceedings of the Thirty-First Hawaii International Conference on System sciences; Jan. 6-9, 1998.

Luo, H. et al.; "Self-Securing Ad Hoc Wireless Networks;" Jun. 13, 2003, UCLA Computer Science Dept., Los Angeles, CA.

Will, J.D.; "Wireless Networking for Control and Automation of Off-Road Equipment;" an ASAE Meeting Presentation; Jul. 18-21, 1999; Toronto, Canada.

Zhang, Y. et al.; "Intrusion Detection in Wireless Ad-Hoc Networks;" Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking; Aug. 6-11, 2000.

"Microsoft Announces Wireless Provisioning Services;" GeekZone; Wi-Fi, posted Dec. 10, 2003 20-56-21 NZ.

Fried, Ina; "HP Spotlights Mobile Gear;" CNET News.com; Oct. 13, 2003.

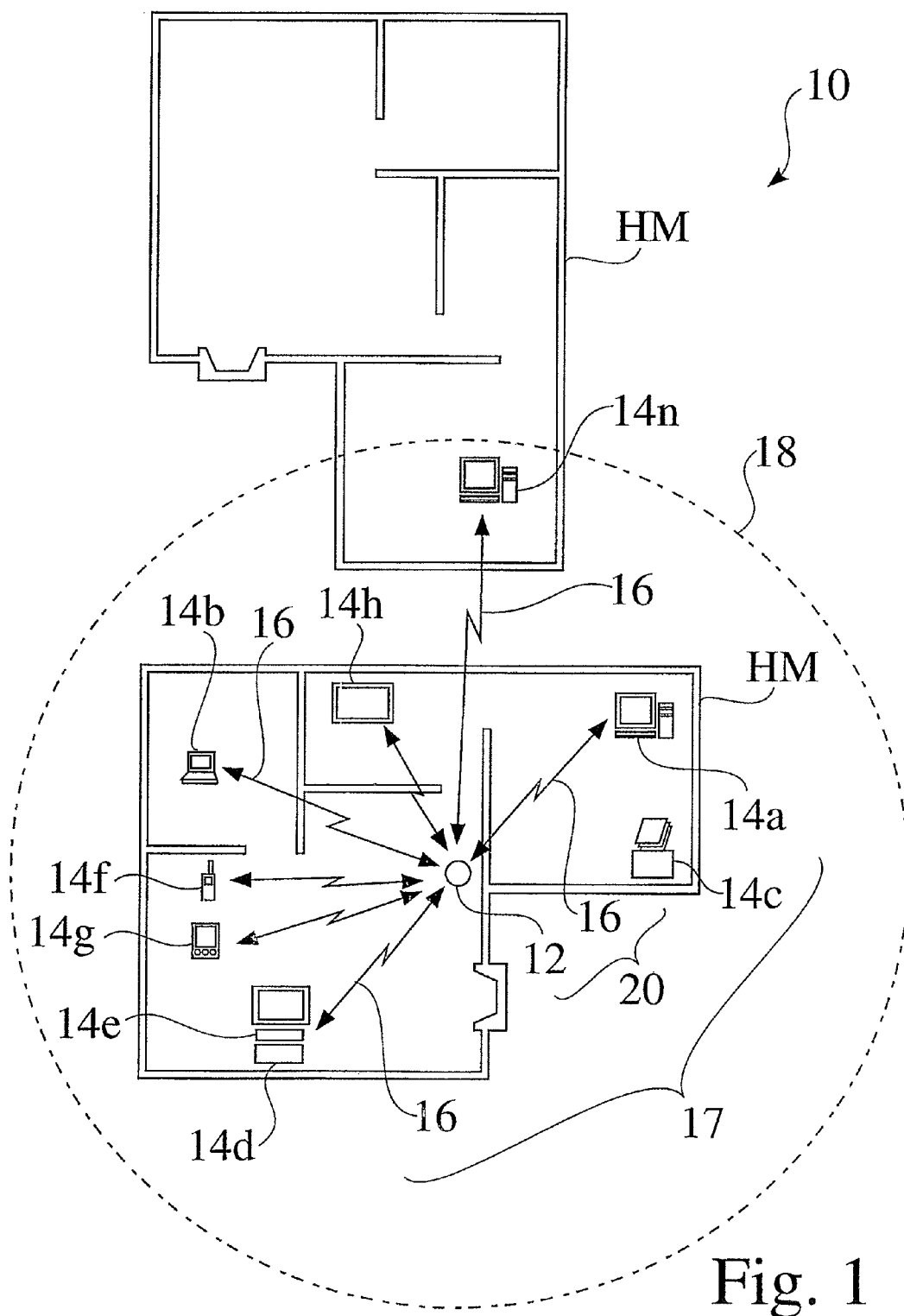
"Wireless Provisioning Services Overview;" The Cable Guy—Dec. 2003, Tech-Net Newsletter; 2004 Microsoft Corporation.

Sony Ericsson Mobile Communications; Sony Ericsson HBH-65 (Manual); Pub # LZT 1086746 RIA; 1.sup.st Ed. Aug. 2003; Sony Ericsson Mobile Communications, AB.

International Search Report and Written Opinion, issued in International Patent Application No. PCT/US2004/000860, mailed Aug. 17, 2004, 5 pages.

International Preliminary Report on Patentability, issued in International Patent Application No. PCT/US2004/000860, mailed Jul. 15, 2005, 4 pages.





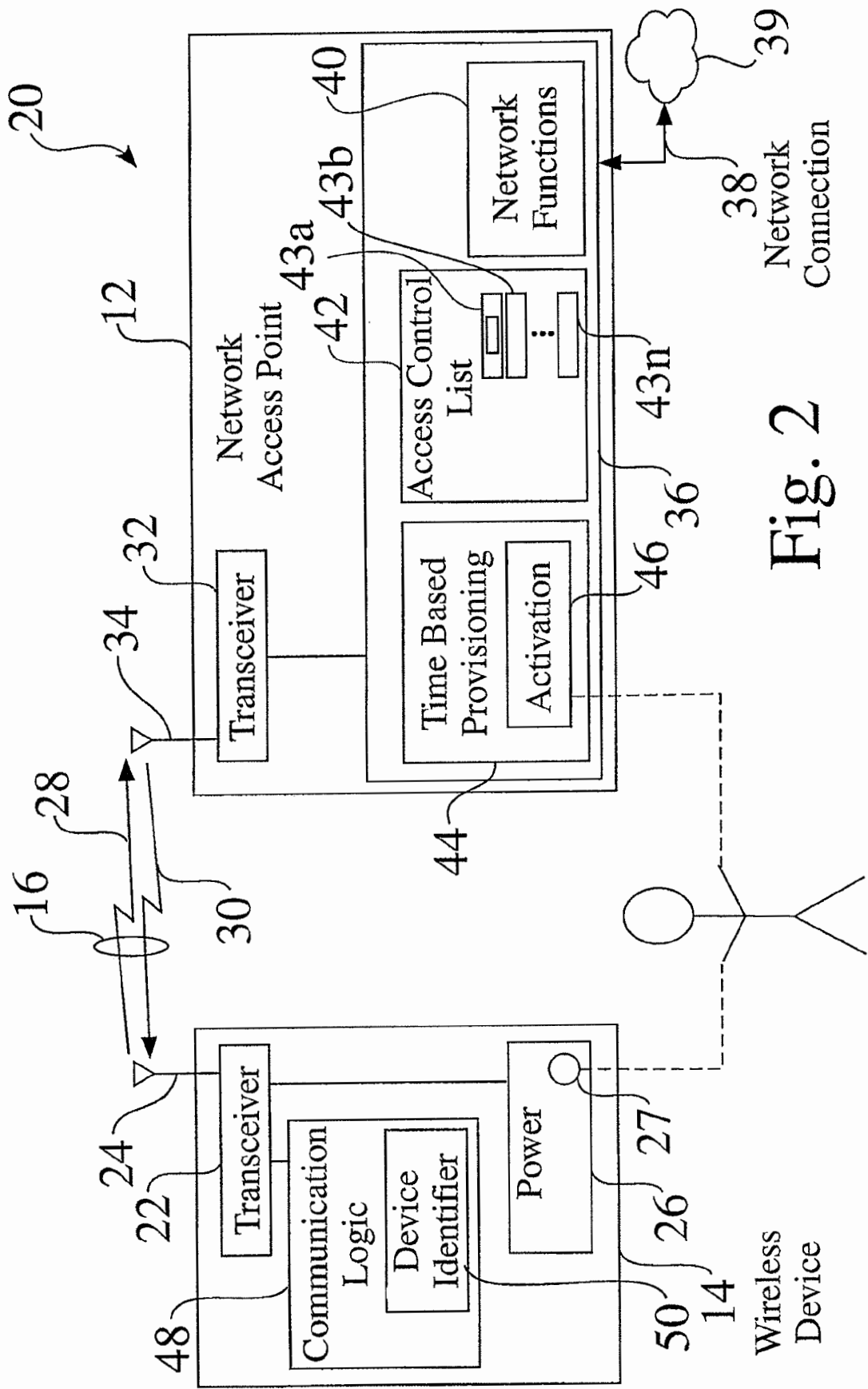


Fig. 2

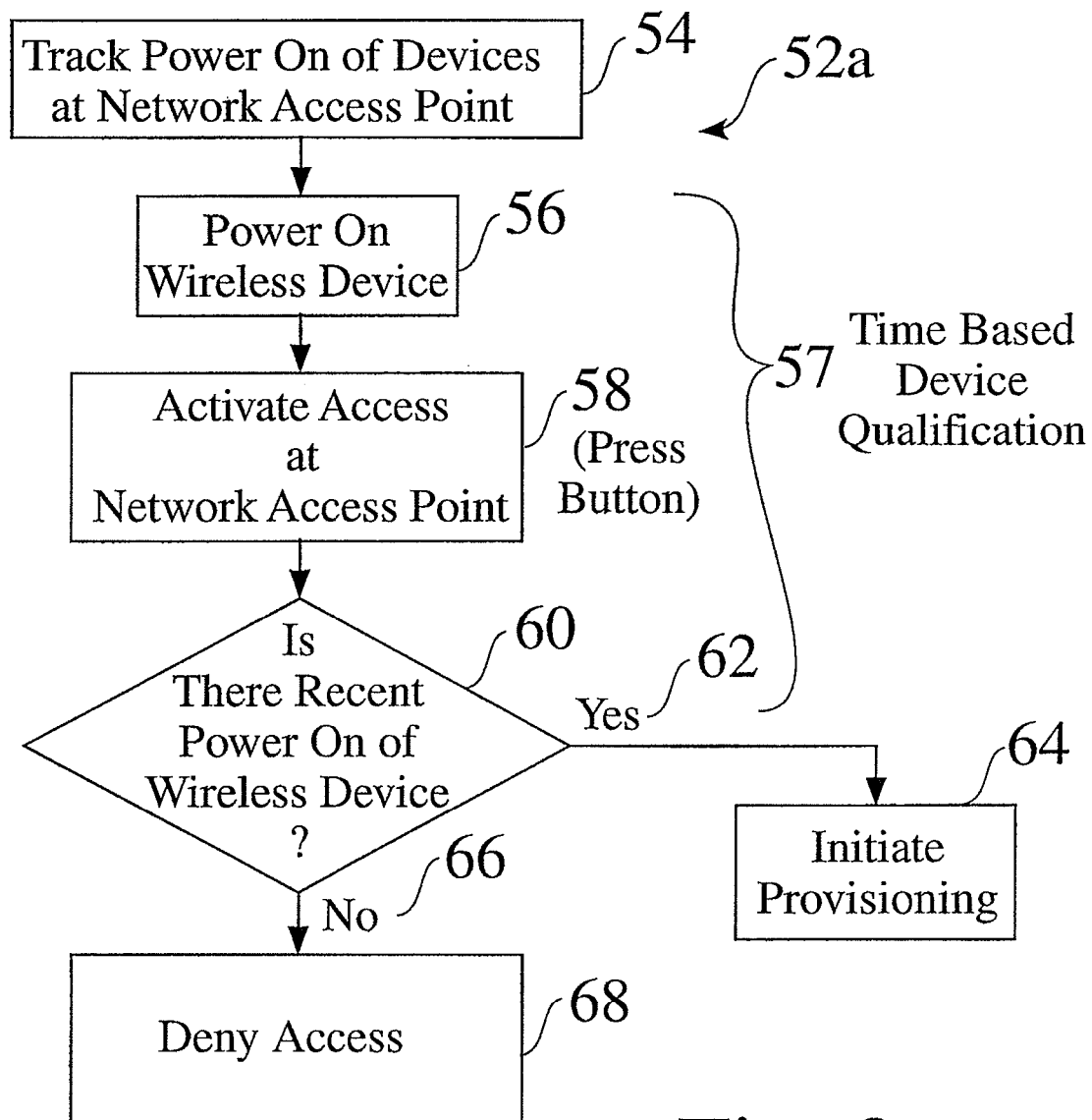


Fig. 3

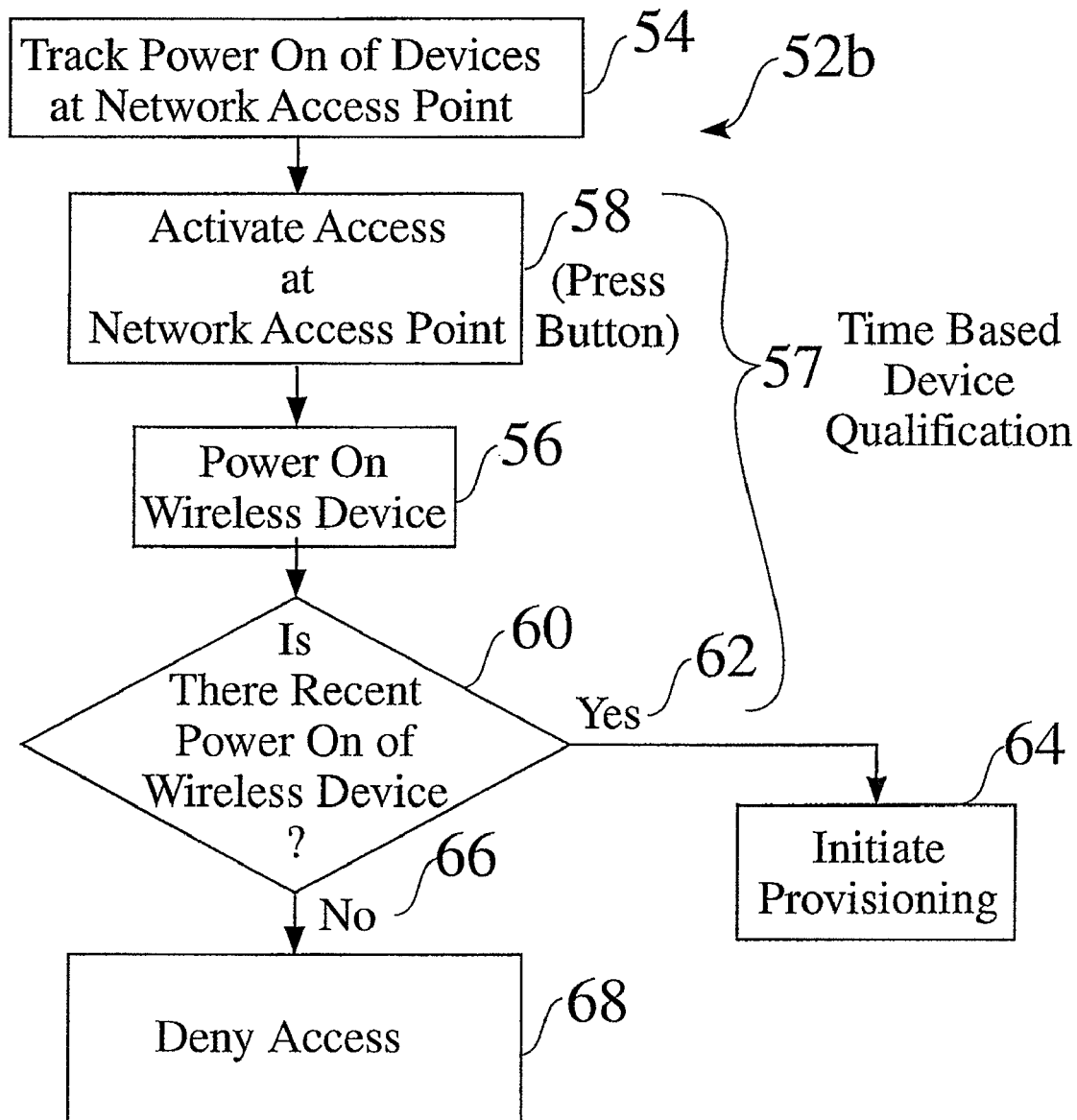
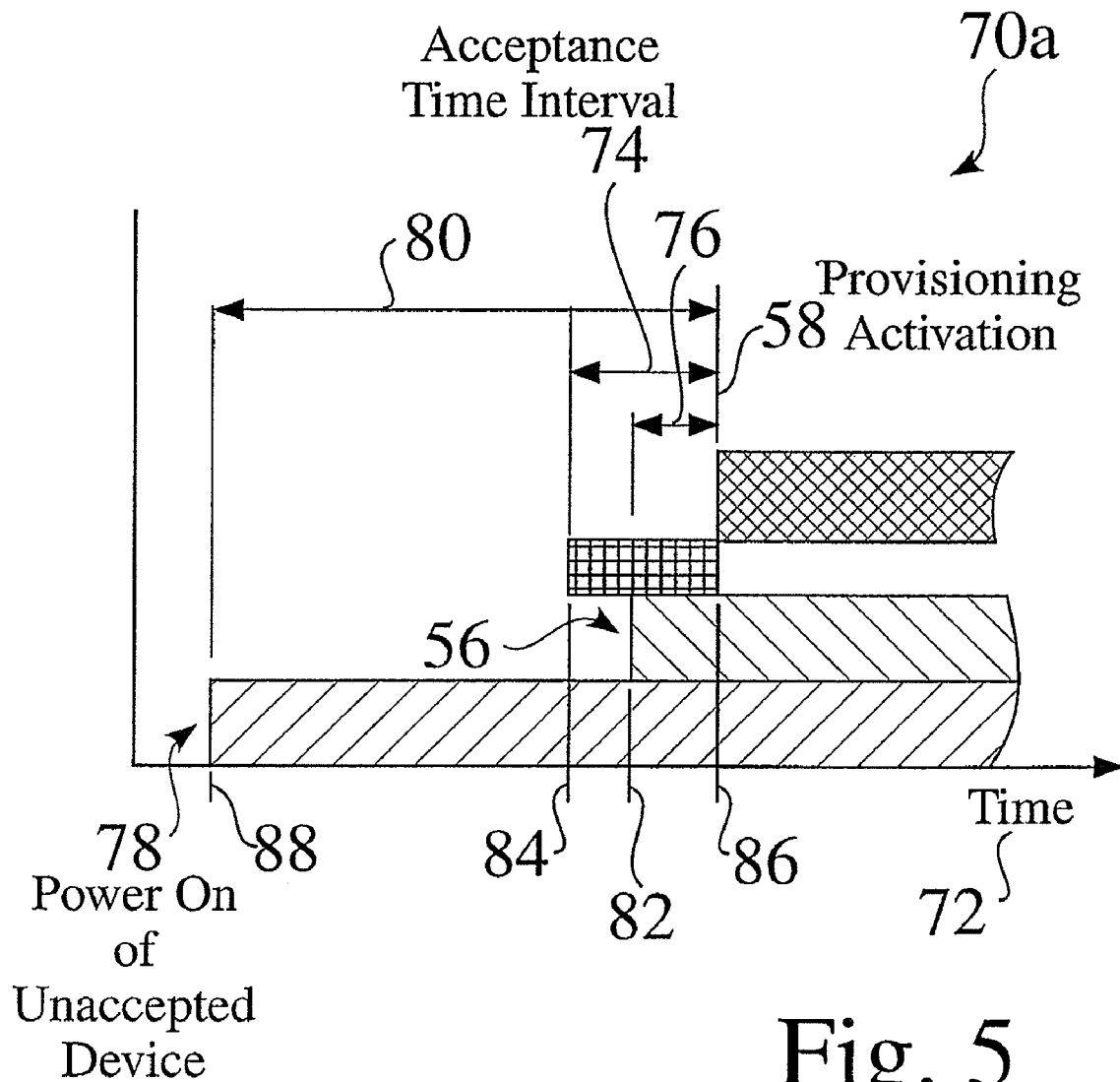


Fig. 4



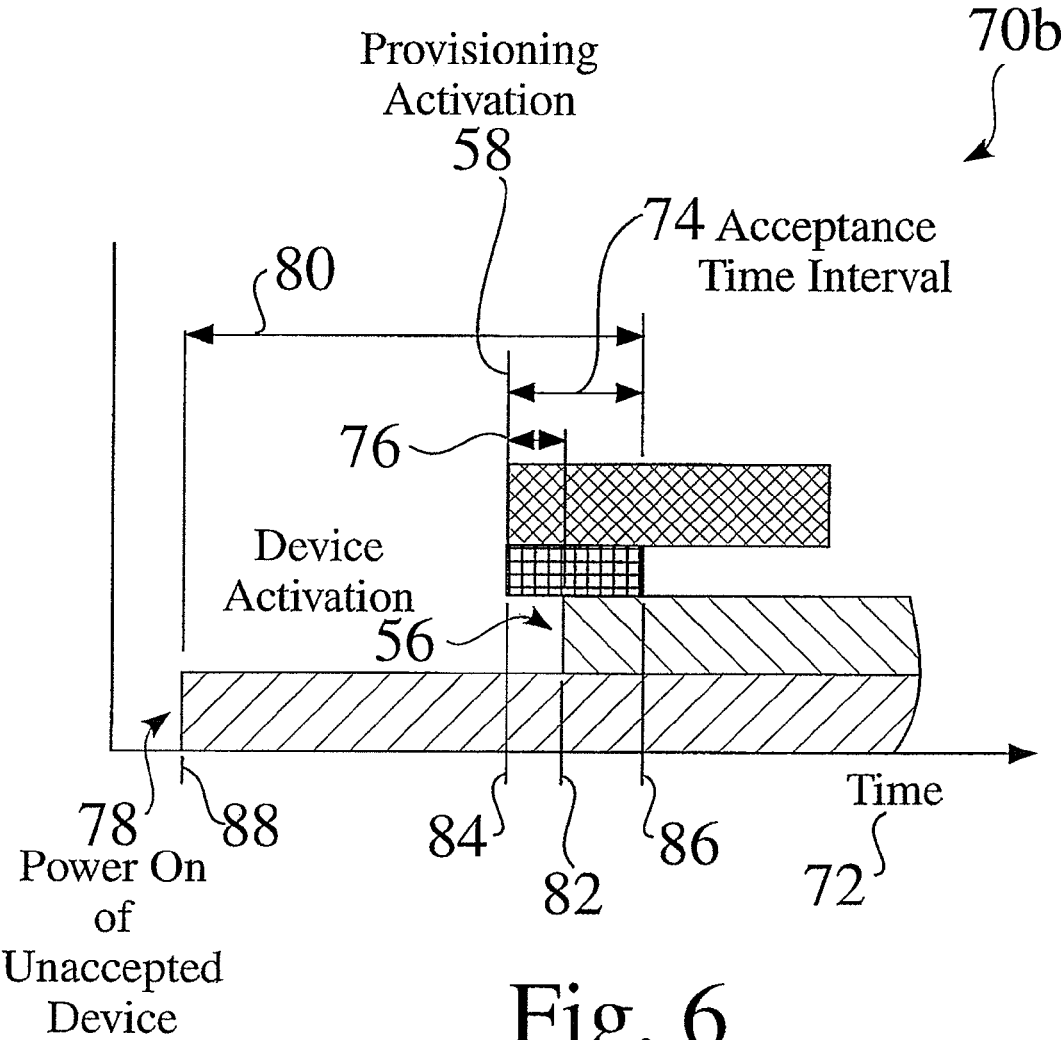


Fig. 6



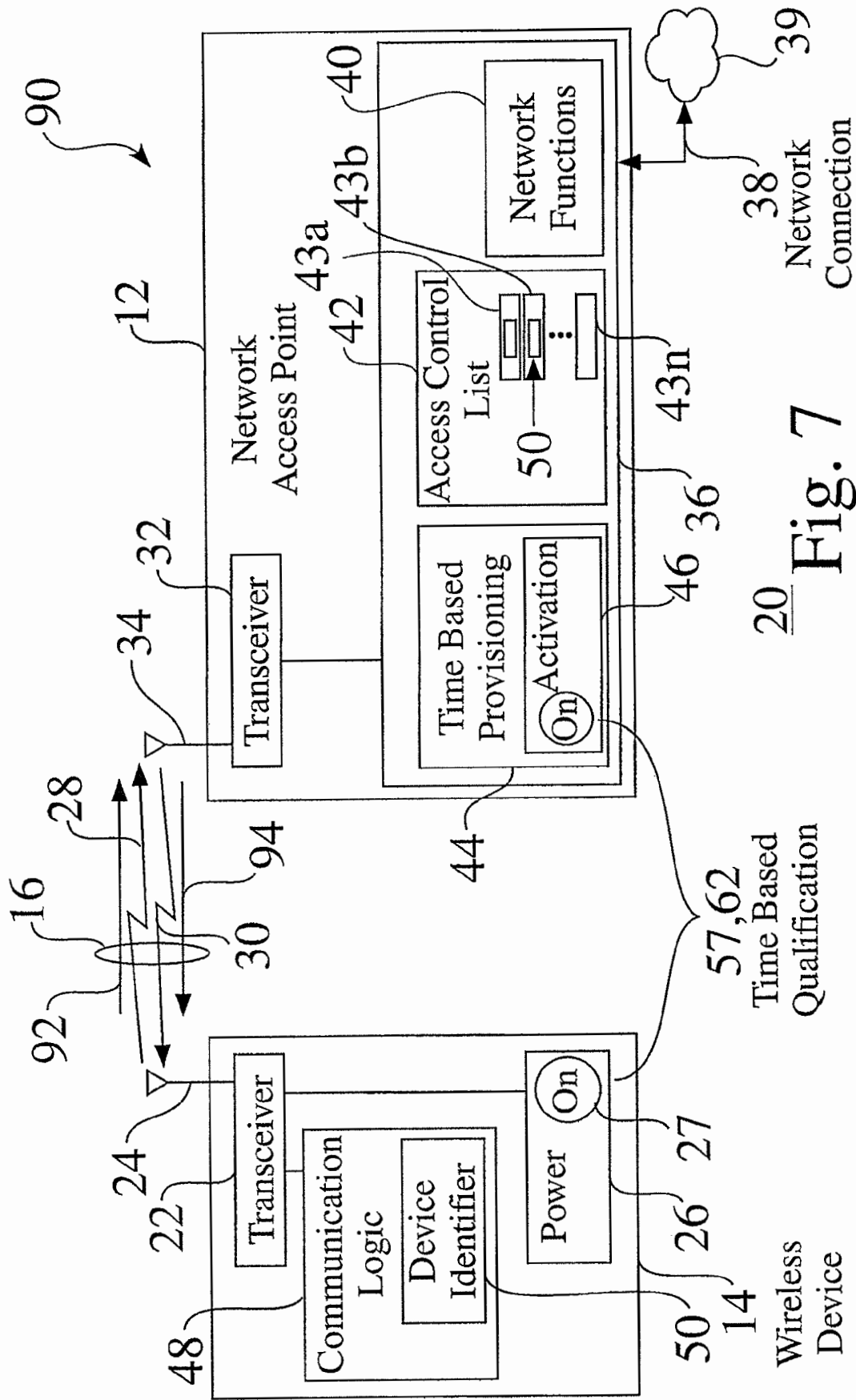


Fig. 7

US 7,911,979 B2

1

**TIME BASED ACCESS PROVISIONING  
SYSTEM AND PROCESS****CROSS REFERENCE TO RELATED  
APPLICATIONS**

This application is a Continuation of and claims priority to U.S. Ser. No. 11/673,513, filed 9 Feb. 2007, which is a Continuation of and claims priority to U.S. Ser. No. 10/961,959, filed 8 Oct. 2004, which was issued as U.S. Pat. No. 7,177,285 on 13 Feb. 2007, which is a Continuation of and claims priority to U.S. Ser. No. 10/341,847, filed 13 Jan. 2003, which was issued as U.S. Pat. No. 6,891,807 on 10 May 2005, each of which are incorporated herein in their entirety by this reference thereto.

This Application is also related to PCT Application No. PCT/US04/00860, filed 13 Jan. 2004, which claims the benefit of U.S. Ser. No. 10/341,847, filed 13 Jan. 2003, which was issued as U.S. Pat. No. 6,891,807 on 10 May 2005.

**FIELD OF THE INVENTION**

The invention relates to the field of wireless connections between a wireless device and a network. More particularly, the invention relates to access provisioning between one or more wireless devices and an intranet access point.

**BACKGROUND OF THE INVENTION**

In local area networks, such as wireless home networks, one or more wireless devices, e.g. such as IEEE 802.11b devices, are linked to the network by a provisioning process through a network access point. When a user acquires a new wireless device, they need to securely tie it to their intranet, which comprises telling the intranet to accept wireless communications from the device, as well as provisioning the device with key material, such as for creating an encrypted connection. In conventional networks having one or more devices to be provisioned to a network access point, device identification information, such as a MAC address, is required to be communicated from the wireless device to the access point. Several methods have been described for wireless access provisioning to integrate wireless devices into a network.

M. Cudak, B. Mueller, J. Kelton, and B. Glasson, Network Protocol Method, Access Point Device and Peripheral Devices for Providing for an Efficient Centrally Coordinated Peer-to-Peer Wireless Communications Network, U.S. Pat. No. 6,058,106, disclose a "peer-to-peer wireless communications network wherein the access point device: (1) broadcasts a block assignment that specifies a wireless source peripheral device and a wireless destination peripheral device; (2) receives, from the wireless destination peripheral device, sequence information; (3) determines whether the sequence information represents one of: a negative acknowledgment and a positive acknowledgment with a sequence number; (4) forwards an acknowledgment to the wireless source peripheral based on the sequence information, and repeats steps (1)-(4) until N blocks of data, N a predetermined integer, have been transferred from the wireless source peripheral to the wireless destination peripheral."

J. Lin, P. Alfano, and S. Upp, Method and Apparatus for Performing Bearer Independent Wireless Application Service Provisioning, U.S. Pat. No. 6,275,693 disclose a provisioning system, in which a "mobile communication device contacts a provisioning proxy over the wireless bearer network, which in turns contacts a provisioning center over a public network.

2

A provisioning tunnel is then established between the provisioning center and the mobile communication device. Once the provisioning tunnel is set up, the user of the mobile communication device can subscribe to, or unsubscribe from wireless application services."

Wireless Device Registering Method in Wireless Home Network, PCT Patent Application No. WO 01/2266, describes the sending of an authentication key to a device for storage, when an identification code received from the device corresponds to a code stored in an access point.

Secure Wireless LAN, European Pat. No. EP, 1081895, discloses wireless device use by a wireless device operator with an access point connected to a wired LAN in communication with the wireless device through air channel authentication.

C. Candolin, *Security Issues for Wearable Computing and Bluetooth Technology*, 23 Oct. 2000, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, P.B. 400, FIN-02015 HUT, Finland, describes Bluetooth Technology as "a short-range wireless cable replacement technology enabling restricted types of ad hoc networks to be formed. All the while, a need for connecting wearable devices, such as PDAs, mobile phones, and mp3-players, is rising. Such networks may be formed using Bluetooth technology, but issues such as security must be taken into consideration. Although an attempt to tackle security is made, the result is too weak to be used for anything else than for personal purposes."

Other systems provide various details of the operation of wireless devices within a network, such as U.S. Pat. No. 6,418,324, Apparatus and Method for Transparent Wireless Communication; U.S. Pat. No. 6,418,146, Integrated Communication Center Functionality for WAP Devices; U.S. Pat. No. 6,359,880, Public Wireless/Cordless Internet Gateway; U.S. Pat. No. 6,334,056, Secure Gateway Processing for Handheld Device Markup Language; U.S. Pat. No. 6,317,594, System and Method for Providing Data to a Wireless Device Upon Detection of Activity of the Device on a Wireless Network; U.S. Pat. No. 6,282,183, Method for Authorizing Coupling between devices in a Capability Addressable Network; U.S. Pat. No. 6,272,129, Dynamic Allocation of Wireless Mobile Nodes Over An Internet Protocol (IP) Network; U.S. Pat. No. 6,167,428, Personal Computer Microprocessor Firewalls for Internet Distributed Processing; European Pat. No. 1225778, Wireless Repeater Using Identification of Call Originator; European Pat. No. EP 1191763, Access Authentication System for a Wireless Environment; European Pat. No. 1126681, A Network Portal System and Methods; European Pat. No. EP1081895, Secure Wireless Local Area Network; European Pat. No. EP 999672, System and Method for Mapping Packet Data Functional Entities to Elements in a Communications Network; European Pat. No. EP814623, Mobile Decision Methodology for Accessing Multiple Wireless Data Networks; *Privacy and Authentication for Wireless Local Area Networks*, Ashar Aziz and Whitfield Diffie, Sun Microsystems, Inc., Jul. 26, 1993; *Painting Your Home Blue (Bluetooth™ Wireless Technology)*, D. Cypher, Proceedings 2002 IEEE 4<sup>th</sup> International Workshop on Networked Appliances, Jan. 15-16, 2002; *Wireless Home Networks on a Hierarchical Bluetooth Scatternet Architecture*, W. Lilakiatsakun, A. Seneviratne, Proceedings Ninth IEEE International Conference on Networks, Oct. 10-12, 2001; *Bluetooth Wireless Technology in the Home*, R. Shephard, Electronics & Communication Engineering Journal; October 2001; *Wireless Gateway for Wireless Home AV Network and It's Implementation*, T. Saito, I. Imoda, Y. Takabake, K. Teramoto, and K. Fujimoto, IEEE Transactions on

US 7,911,979 B2

3

Consumer Electronics, August 2001; *A Wireless Home Network and its Applications Systems*, H. Fujieda, Y. Horiike, T. Yamamoto, and T. Nomura, IEEE Transactions on Consumer Electronics, May 2000; *Wireless Home Link*, M. Nakagawa, IEICE Transactions on Communications, December 1999; *An Access Protocol for a Wireless Home Network*, A. C. V. Gummalla, and J. O. Limb, WCNC 1999 IEEE Wireless Communications and Networking Conference; Sep. 21-24, 1999; *Firewalls for Security in Wireless Networks*, U. Murthy, O. Bukres, W. Winn, and E. Vanderdez, Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Jan. 6-9, 1998; *Self-Securing Ad Hoc Wireless Networks*, Haiyun Luo, Petros Aertfos, Jiejun Kng, Songwu Lu, and Lixia Zhang; *Wireless Networking for Control and Automation of Off-Road Equipment*, J. D. Will; ASAE Meeting Presentation; and *Intrusion Detection in Wireless Ad-Hoc Networks*, Yongguang Zhang and Wenke Lee, Proceeding of the Sixth Annual International Conference on Mobile Computing and Networking, Aug. 6-11, 2000.

The disclosed prior art systems and methodologies thus provide basic provisioning for wireless devices to a network through an access point. However, for many networks, such provisioning schemes are often impractical, either for wireless devices which lack a user interface which is configured for communicating provisioning information, or for simple home-based intranets. For example, device identification information, such as a MAC address, is often required to be manually transcribed from the wireless device to the access point, since wireless devices often lack a user interface control to reveal such identifying information. For example, a wireless picture frame device typically lacks a control interface to read or extract identification information, such as a MAC address.

While some wireless devices include a user interface for dedicated device functionality, e.g. such as a user control for a game box or a digital video recorder, a dedicated user interface is often incapable or cumbersome to be used to communicate device identification and to exchange provisioning information. In addition, while some wireless devices provide a user interface control which can reveal such identifying information, provisioning procedures still require a user to be technically proficient to properly initiate and complete a provisioning process.

It would therefore be advantageous to provide a network provisioning system, which does not require a user interface for the initiation of a provisioning process. The development of such a wireless access provisioning system would constitute a major technological advance.

Furthermore, it would be advantageous to provide a wireless access provisioning structure and process with minimal device requirements and/or user proficiency, whereby a wireless device is readily provisioned by the provisioning system, and whereby other devices within an access region are prevented from being provisioned by the provisioning system. The development of such a provisioning system would constitute a further technological advance.

As well, it would be advantageous that such a wireless access provisioning system be integrated with easily monitored parameters of a wireless device, such as the time monitoring of power on and/or start of signal transmission. The development of such a provisioning system would constitute a further major technological advance. The development of such a time-based wireless access provisioning system for provisioning secure encrypted communication would constitute a further technological advance.

#### SUMMARY OF THE INVENTION

A method and apparatus is provided for the time-based provisioning of wireless devices. A network access point

4

monitors operation of wireless devices within a service region. When provisioning logic is activated at the network access point, the access point determines if the tracked parameter, such as the power on, of the wireless device occurs within a designated time interval from the time of the provisioning activation. If the tracked device qualifies, the network access point proceeds with provisioning the device. When a wireless device to be authorized is powered on, the provisioning logic at the network access point notes the power on time. The user then activates the provisioning access at the network access point, and the network access point provisions the wireless device if it is recently powered on.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic plan view of a time based wireless access provisioning system;

FIG. 2 is a functional block diagram of a time based wireless access provisioning system;

FIG. 3 is a flow chart of a time based wireless access provisioning process;

FIG. 4 is a flow chart of an alternate time based wireless access provisioning process;

FIG. 5 shows a simplified timeline for a time based wireless access provisioning process;

FIG. 6 shows a simplified timeline for an alternate time based wireless access provisioning process; and

FIG. 7 shows the time-based acceptance and provisioning of a new wireless device within a time based wireless access provisioning system.

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 is a schematic plan view 10 of a time based wireless access provisioning system 20. FIG. 2 is a functional block diagram of a time based wireless access provisioning system 20, comprising a network access point 12 adapted to provide time-based provisioning with a wireless device 14.

The network access point 12 shown in FIG. 2 comprises a transceiver 32 and antenna 34, which provides communication 16 to one or more wireless devices 14. The communications channel 16 typically comprises an input, i.e. reverse link, signal 28 from a wireless device 14 to the access point, as well as an output, i.e. forward link, signal 30, from the access point 12 to the wireless device 14.

As seen in FIG. 2, the network access point 12 typically comprises network logic and componentry 36, such as networking functions 40, thereby providing communications between one or more authorized wireless devices 14 and a local network 17 (FIG. 1). The network access point 12 shown in FIG. 2 also comprises a network connection 38 to one or more networks 39, such as to wired devices within a LAN, and/or to other networks, such as the Internet. The network access point 12 shown in FIG. 2 comprises an access control list 42, which identifies wireless devices 14 which have proper access to the local network 17 (FIG. 1), such as by storing accepted device identifications 50 as list elements 43a-43n.

The wireless device 14 shown in FIG. 2 comprises a device transceiver 22 and antenna 24, which provides communication 16 to the network access point 12, and in some embodiments to other wireless devices 14. The wireless device 14 comprises communication logic and componentry 48, and comprises an associated device identifier 50, e.g. such as a unique MAC address, which is communicatable to the network access point 12, whereby the wireless device 14 can be

US 7,911,979 B2

5

controllably provisioned into the network 17 by the network access point 12. The wireless device 14 also comprises power 26, e.g. wired or battery, and power activation 27. In some embodiments of the time based wireless access provisioning system 20, the wireless device 14 is an IEEE 802.11 WLAN and/or Bluetooth™ compliant device.

The network access point 12 shown in FIG. 1 is located within a service area 18 for a network 17, such as a wireless local area network (WLAN) or a wireless personal area network (WPAN), and typically communicates 16 with a one or more wireless devices 14 which operate within the service area 18, as well as to other wired devices connected to the network, and to connected 38 networks 39, such as the Internet.

As seen in FIG. 1, the time based wireless access provisioning system 20 can be used for a wide variety of wireless devices 14a-14n which are adapted to communicate with the network access point 12, such as but not limited to a desktop computer 14a, a portable laptop computer 14b, a network printer 14c, a digital video recorder 14d, a game box 14e, a portable phone 14f, a personal digital assistant (PDA) 14g, and/or a wireless picture frame 14h.

The network access point 12 provides time-based provisioning to ensure that only authorized wireless devices 14 can operate within the local network 17, such as within a home HM, and to prevent unauthorized wireless devices 14, such as device 14n in FIG. 1, from gaining access to the network 17.

In the time based wireless access provisioning system 20, the network access point 12 also comprises time based provisioning 44, which is activatable 46, such as manually by a user U. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17. A properly timed interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12 acts to qualify the wireless device 14 to the network access point.

Time-Based Provisioning Process. FIG. 3 is a flow chart of a time based wireless access provisioning process 52a. The network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 5). The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46.

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 3, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, e.g. such as within 5 minutes. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 5), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 3, the time based wireless access provisioning process 52a also prevents network access from devices 14 which are powered on 78 (FIG. 5) at an earlier time 88 (FIG. 5). If a wireless device 14 is powered on at a time 88 before the acceptance time interval 74 (FIG. 5), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device, preventing provisioning 64 into the network 17.

FIG. 5 shows a simplified timeline 70a for a time based wireless access provisioning process 52a. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 5, the network access point 14 notes the start time 82 of the power on 56 of a

6

wireless device 14 which is desired to be provisioned within the network 17. The user then activates provisioning logic 44 at the network access point 12, at time 86. The provisioning logic 44 typically comprises an acceptance time interval 74, e.g. such as a 5 minute interval 74, having a start time 84 and an end time 86, within which desired devices 14 are accepted 62 (FIG. 3). As seen in FIG. 5, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 5, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned by the network access point 12. When the user activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, i.e. failing 66 time-based determination 60 (FIG. 3) such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Alternate Time-Based Provisioning Process. FIG. 4 is a flow chart of an alternate time based wireless access provisioning process 52b, in which a desired wireless device 14 to be provisioned is powered on after the provisioning logic 44 is activated. As above, the network access point 12 tracks 54 the power on time of wireless devices 14, whereby the powered wireless device begins transmission of a reverse link signal 28. The user U then activates 58 the provisioning access 44 at the network access point 12, typically by pressing an activation button or switch 46. When a wireless device 14 to be authorized is powered on 56, the provisioning logic 44 at the network access point 12 notes the power on time 82 (FIG. 6).

In response to a properly timed interaction 57, the network access point 12 provisions the wireless device 14 automatically. As seen in FIG. 4, the network access point 12 determines 60 if there is a recent power on of a wireless device 14, after the provisioning logic 44 is activated 58. If the wireless device 14 was recently powered 56, such as within an acceptance time interval 74 (FIG. 6), the positive determination logic 62 allows the network access point 12 to initiate provisioning 64.

As seen in FIG. 4, the alternate time based wireless access provisioning process 52b also prevents network access from devices 14 which are powered on 78 (FIG. 6) at an earlier time 88 (FIG. 6). If a wireless device 14 is powered on at a time 88 before (or after) the acceptance time interval 74 (FIG. 6), the negative determination logic 66 allows the network access point 12 to deny access 68 to the device 14, preventing provisioning 64 into the network 17.

FIG. 6 shows a simplified timeline 70b for the alternate time based wireless access provisioning process 52b. The enhanced network access point 12 tracks power on 56 of wireless devices as a function of time 72. As seen in FIG. 6, the user activates provisioning logic 44 at the network access point 12, at time 84. The network access point 14 notes the start time 82 of the power on 56 of a wireless device 14 which is desired to be provisioned within the network 17. If the power on 56 falls within the acceptance time interval 74, the desired device 14 is accepted 62 (FIG. 4). As seen in FIG. 6, the time interval 76 for the desired device 14 properly falls within the acceptance interval 74, such that the provisioning logic 44 accepts 62 the wireless device 14, and initiates provisioning 64.

As further seen in FIG. 6, the network access point 14 also notes the start time 88 of the power on 78 of a second wireless device 14, which is not necessarily desired to be provisioned



US 7,911,979 B2

7

by the network access point 12, such as from an unauthorized device 14, or from a desired device which is not powered on within the time interval 74. When the user then activates the provisioning logic 44 at the network access point 12, at time 86, the time interval 80 for the second device 14 falls outside the acceptance interval 74, and before the activation 58 of the provisioning logic 44, such that the provisioning logic 44 denies 68 the second wireless device 14, and prevents provisioning 64.

Device Qualification. FIG. 7 provides a schematic view 90 of a time-based acceptance of a new wireless device 14 within a time based wireless access provisioning system 20.

When the provisioning logic 44 time-qualifies 62 (FIG. 3, FIG. 4) a wireless device 14, the wireless access point 12 accepts the time-based qualification 57, and initiates the provisioning process 64, which typically comprises communication 16 and secure provisioning of information between the wireless device 14 and the network access point 12, such as the exchange of key material, if an encryption protocol is to be used. Device parameters, such as the device identifier 50, are typically sent 92 to the access point 12, wherein the device identifier 50 is added to the network access control list 42. As seen in FIG. 7, the device identifier 50 for the accepted wireless device 14 is added to the access control list 42, such as an element 43b in the list of qualified devices 14. Provisioning information may also be sent 94 from the network access point 12 to the device 14, such as to establish setup, handshaking, or encryption provisioning.

System Implementation. The time-based wireless access provisioning system 20 readily integrates one or more wireless devices 14 into a local area network in a secure fashion. For example, when a user U brings home a new wireless device 14 for use in their existing home network 17, the time-based wireless access provisioning system 20 allows the user U to easily add the new device to the network 17, without exposing the network unnecessarily to attack from third parties.

Within the time based access provisioning system 20, the enhanced network access point 12 keeps track of all wireless devices 14a-14n in the vicinity 18 of the central access point 12. The time based wireless access provisioning system 20 securely integrates one or more wireless devices 14 into the local area network 17, based upon a properly timed device qualification interaction 57 (FIG. 3, FIG. 4) between a wireless device 14 to be provisioned and the network access point 12.

As seen in FIG. 3 and FIG. 4, when a user U brings a device 14 home HM and powers on the wireless device 14, the user then simply presses a button 46 on their network access point 12. In response thereto, the access point 12 provisions the wireless device automatically, based on the time-based qualification 57. Since the access point 12 is only available for such provisioning for a short interval 74 after the button 46 is pressed, it is unlikely that the access point 12 will provision unauthorized third party devices 14.

The qualification protocol 52a, 52b allows the network access point 12 to augment the access control list 42 with a properly qualified device 14. The network access point can discount, i.e. deny, devices in neighboring residences HM that have been on for a long time, wherein power on 78 of the devices 14 extends beyond the acceptance interval 74, and can identify and provision one or more devices 14 that are powered on 56 within the acceptance interval 74.

The time-based access provisioning system 20 does not require a user interface on a wireless device 14 to initiate device setup and provisioning. As the power on or beginning of signal transmission 16 is easily tracked by the enhanced

8

network access point 12, a simple activation 46, such as the pushing of a button 46, can be used to time-qualify 57 a desired device 14, and to deny qualification 66 for an unqualified device. Therefore, the time-based access provisioning system 20 drastically simplifies wireless setup and provisioning for wireless devices. Wireless devices 14 to be provisioned are not required to have complex user interfaces, and users are not required to perform complex provisioning procedures. The time-based access provisioning system 20 simplifies the integration of wireless devices into a network, and provides more than reasonable levels of security.

Alternate Applications for the Time-Based Access Provisioning System.

While the time based access provisioning system 10 is disclosed above as tracking a single power on 56, 78 of wireless devices, alternate embodiments of the time based access provisioning system 10 provide further network protections from undesired devices.

For example, for a neighboring device which is switched on and off repeatedly, such as for an undesired wireless device or user in search of a network access point 12, the network access point 12 tracks the repeated powering operation, and can deny provisioning access as desired.

Although the time based access provisioning system and its methods of use are described herein in connection with wireless devices, personal computers and other microprocessor-based devices, such as wireless appliances, the apparatus and techniques can be implemented for a wide variety of electronic devices and systems, or any combination thereof, as desired.

Furthermore, while the time based access provisioning system and its methods of use are described herein in connection with wireless devices and intranets or LAN's, the apparatus and techniques can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

As well, while the time based access provisioning system and its methods of use are described herein in connection with a time based interaction between a wireless device and a network access point, the use of tracking power on/off as a signal to associate devices automatically can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.

The invention claimed is:

1. A provisioning process performed by a provisioning system having provisioning logic, comprising:

tracking, by the provisioning logic, an operating parameter of a first device, wherein the operating parameter of the first device comprises any of a power on of the first device, and an onset of a signal transmission of the first device; and

sending a signal to initiate provisioning of the first device with a network if the tracked operating parameter occurs within a designated time interval.

2. The process of claim 1, wherein the first device is an IEEE 802.11 compliant wireless device.

3. The process of claim 1, wherein the first device is a BLUETOOTH™ compliant device.

4. The process of claim 1, wherein the initiation of provisioning is prevented if any of the tracked operating parameter occurs repeatedly, and the tracked operating parameter occurs

outside the time interval, comprising any of before the time interval and after the time interval.

5. The process of claim 1, wherein at least one other device is associated with the network.

6. The process of claim 5, wherein the network comprises any of an intranet, a local area network, a wireless local area network, and a wireless personal area network.

7. The process of claim 1, wherein the provisioning comprises any of receiving provisioning information and transmitting provisioning information to the first device, wherein the provisioning information includes any of setup information, handshaking information, and encryption information.

8. The process of claim 1, wherein the provisioning comprises receiving a device identifier from the first device and provisioning the first device based on the device identifier address.

9. The process of claim 1, wherein the provisioning comprises receiving a MAC address from the first device and storing the MAC address to an access control list.

10. The process of claim 1, wherein the process is performed on a network access point.

11. The process of claim 1, wherein the operating parameter is an onset of a reverse link signal transmission.

12. The process of claim 1, wherein the designated time interval is based on a user input received by the provisioning logic.

13. The process of claim 1, wherein the designated time interval is a predetermined time period following reception of a user input by the provisioning logic.

14. A system, comprising:  
means for tracking an operating parameter of a first device, wherein the operating parameter of the first device comprises any of a power on of the first device, and an onset of a signal transmission of the first device; and  
means for sending a signal to initiate provisioning of the first device with a network if the tracked operating parameter occurs within a selected time interval.

15. The system of claim 14, wherein the first device is an IEEE 802.11 compliant wireless device.

16. The system of claim 14, wherein the first device is a BLUETOOTH™ compliant device.

17. The system of claim 14, wherein the provisioning comprises reception of a MAC address from the first device and provisioning the first device based on the MAC address.

18. The system of claim 14, further comprising:  
means for activating the selected time interval.

19. A network access device, comprising:  
access control logic configured to:  
track an operating parameter of a first device, wherein the operating parameter of the first device includes any of an indication of a power-on of the first device, and an onset of a signal transmission from the first device; and  
send a signal to initiate provisioning of the first device with a network if the tracked operating parameter occurs within a designated time interval; and  
a transceiver configured to wirelessly communicate with the first device.

20. The network access device of claim 19, further comprising:  
an access control list configured to store identifiers of devices provisioned to wirelessly communicate with the network access device.

21. The network access device of claim 19, further comprising:  
an input configured to receive an indication of a beginning of the designated time interval, wherein the access control logic is further configured to selectively initiate the provisioning of the first device based on whether the tracked operating parameter occurs within a designated time period following reception of the indication.

22. The network access device of claim 19, wherein the first device is an IEEE 802.11 compliant wireless device.

23. The network access device of claim 19, wherein the first device is a BLUETOOTH™ compliant device.

24. The network access device of claim 19, wherein the network is an IEEE 802.11 compliant wireless local area network.

25. The network access device of claim 19, wherein the network is a wireless personal area network.

26. The network access device of claim 19, wherein the operating parameter is an onset of a reverse link signal transmission.

27. A processor-readable storage medium storing non-transitory processor-readable instructions which cause a network access device to perform operations for initiating provisioning of a first device, the operations comprising:  
tracking an operating parameter of the first device, wherein the operating parameter of the first device include any of an indication of a power-on of the first device, and an onset of a signal transmission of the first device; and  
sending a signal to initiate provisioning of the first device with a network if the tracked operating parameter occurs within a designated time interval.

28. The processor-readable storage medium of claim 27, wherein the first device is an IEEE 802.11 compliant wireless device.

29. The processor-readable storage medium of claim 27, wherein the first device is a BLUETOOTH™ compliant device.

30. The processor-readable storage medium of claim 27, wherein the provisioning comprises receiving a device identifier from the first device and provisioning the first device based on the device identifier address.

31. The processor-readable storage medium of claim 27, wherein the operating parameter is an onset of a reverse link signal transmission.

32. The processor-readable storage medium of claim 27, wherein the operations further comprise:  
receiving an indication of a beginning of the designated time interval from an input switch; and  
enabling initiation of device provisioning during the designated time interval.



UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,911,979 B2  
APPLICATION NO. : 12/323399  
DATED : March 22, 2011  
INVENTOR(S) : Roskind et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page 2, item (56), under “Other Publications”, in Column 1, Line 12, delete “Transcations;” and insert -- Transactions; --.

Title Page 2, item (56), under “Other Publications”, in Column 2, Line 25, delete “Ericcson” and insert -- Ericsson --.

Title Page 2, item (56), under “Other Publications”, in Column 2, Line 27, delete “Ericcson” and insert -- Ericsson --.

Column 9, line 51, in Claim 19, delete “power-on” and insert -- power on --.

Column 9, line 56, in Claim 19, delete “interval:” and insert -- interval; --.

Column 10, line 32, in Claim 27, delete “power-on” and insert -- power on --.

Signed and Sealed this  
Nineteenth Day of July, 2011

A handwritten signature in black ink that reads "David J. Kappos". The signature is written in a cursive, flowing style with a large initial "D" and a stylized "K".

David J. Kappos  
*Director of the United States Patent and Trademark Office*

# Exhibit J

---



US007027465B2

(12) **United States Patent**  
**Hautala**

(10) **Patent No.:** **US 7,027,465 B2**  
(45) **Date of Patent:** **Apr. 11, 2006**

(54) **METHOD FOR CONTENTION FREE TRAFFIC DETECTION**

(75) Inventor: **Petri Hautala**, Tampere (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 433 days.

(21) Appl. No.: **10/167,986**

(22) Filed: **Jun. 11, 2002**

(65) **Prior Publication Data**

US 2004/0013134 A1 Jan. 22, 2004

#### Related U.S. Application Data

(63) Continuation of application No. PCT/EP99/10097, filed on Dec. 17, 1999.

(51) **Int. Cl.**  
**H04J 3/07** (2006.01)

(52) **U.S. Cl.** ..... **370/506; 370/350**

(58) **Field of Classification Search** ..... 370/252,  
370/286, 304, 324, 349, 350, 395.43, 444,  
370/506, 509, 512, 229, 230, 230.1, 235,  
370/241

See application file for complete search history.

(56) **References Cited**

#### U.S. PATENT DOCUMENTS

4,627,051 A 12/1986 Shimizu  
4,716,407 A 12/1987 Borrás et al.  
4,930,124 A 5/1990 de Boisseron et al.  
5,594,738 A 1/1997 Crisler et al.

5,675,617 A \* 10/1997 Quirk et al. .... 375/365  
5,678,188 A 10/1997 Hisamura  
5,822,361 A 10/1998 Nakamura et al.  
5,857,092 A \* 1/1999 Nakamura et al. .... 710/62  
5,881,242 A \* 3/1999 Ku et al. .... 709/238  
6,658,363 B1 \* 12/2003 Mejia et al. .... 702/125

#### FOREIGN PATENT DOCUMENTS

EP 0491494 6/1992  
EP 0584667 3/1994  
EP 0749254 12/1996  
EP 0782297 7/1997  
EP 0804006 10/1997  
EP 0917317 5/1999  
EP 0959398 11/1999

#### OTHER PUBLICATIONS

"Wireless LANs and Mobile Networking: Standards and Future Directions" by R.O. LaMaire, et al, IEEE Communications Magazine, 'Online! Aug. 1996, pp. 1-15.

\* cited by examiner

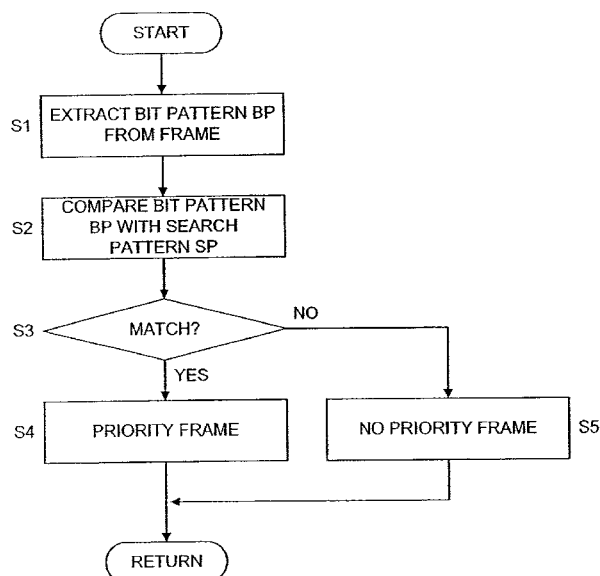
*Primary Examiner*—Dang Ton

*Assistant Examiner*—Phuc Tran

(57) **ABSTRACT**

The invention discloses a method for detecting priority of data frames comprising the steps of extracting (S1) a bit pattern from a predetermined position in a frame, comparing (S2, S3) the extracted bit pattern with a search pattern, and identifying (S4) the received frame as a priority frame in case the extracted bit pattern (BP) matches with the first search pattern (SP). By this method, the priority of a data frame can easily be detected. The invention also proposes a corresponding device for detecting priority of data frames.

**18 Claims, 10 Drawing Sheets**



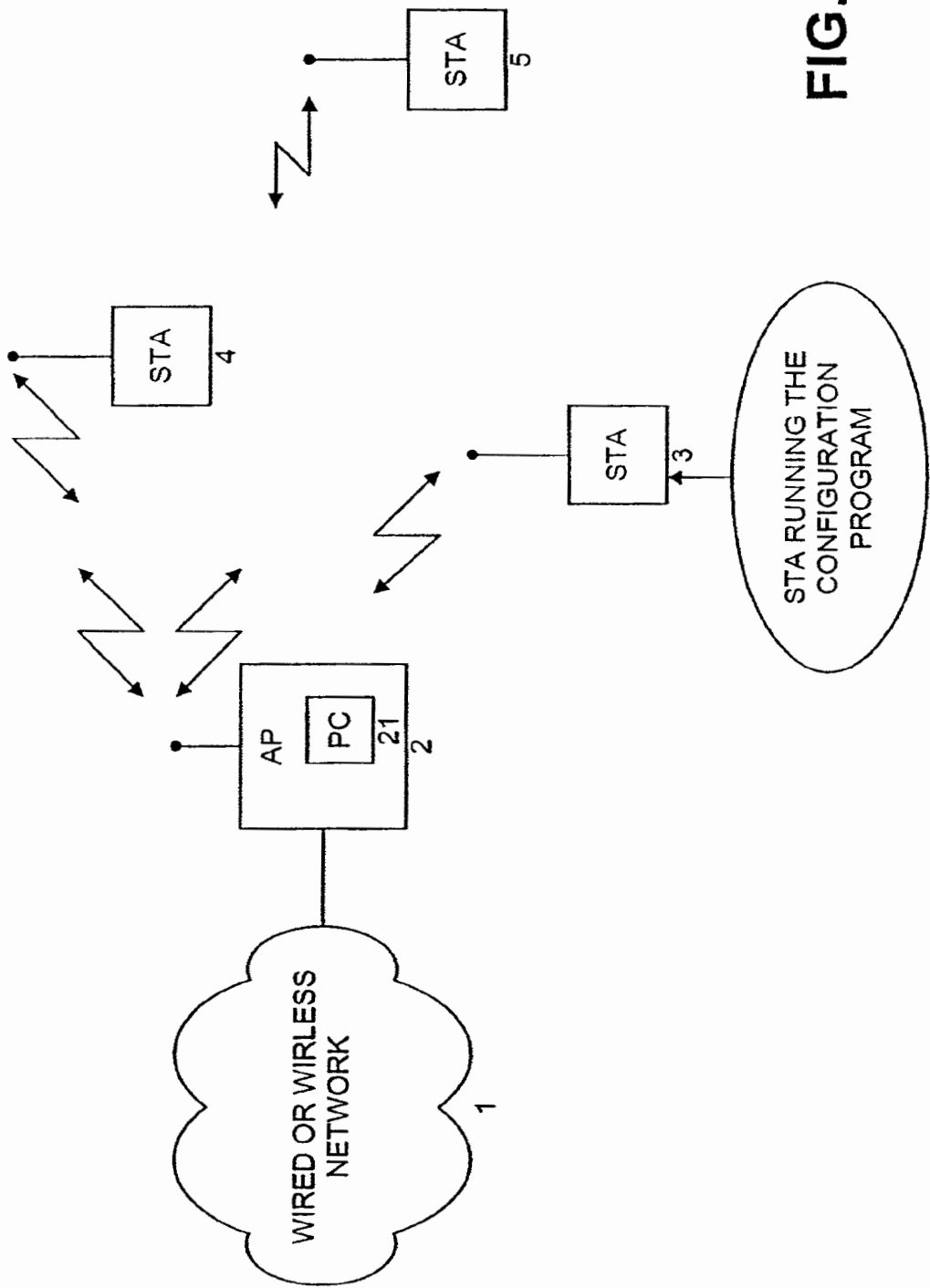


FIG. 1

U.S. Patent

Apr. 11, 2006

Sheet 2 of 10

US 7,027,465 B2

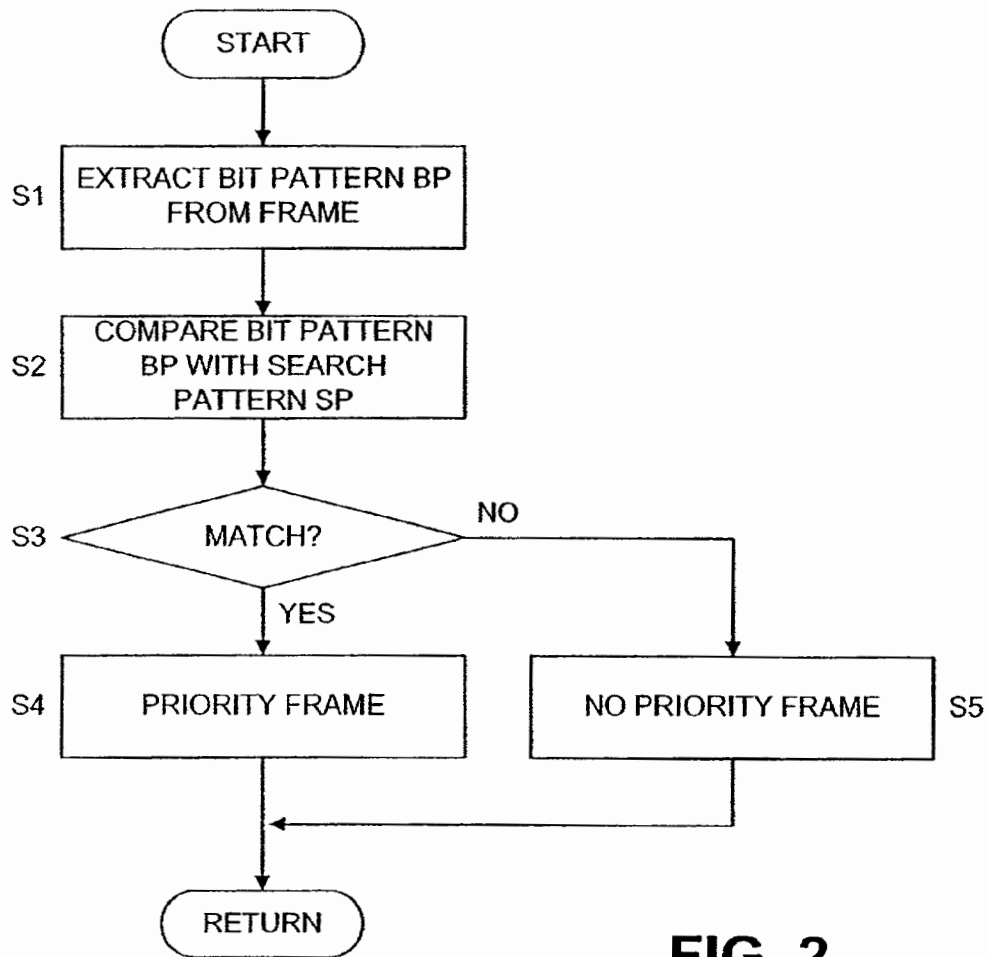


FIG. 2

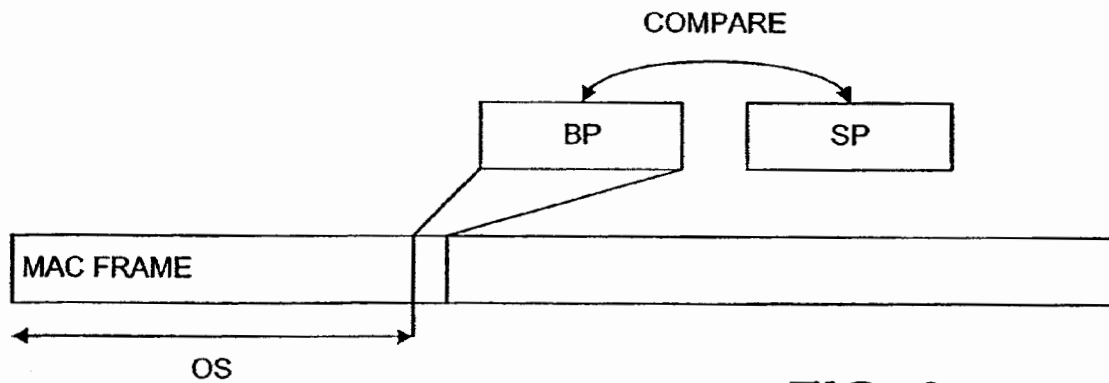
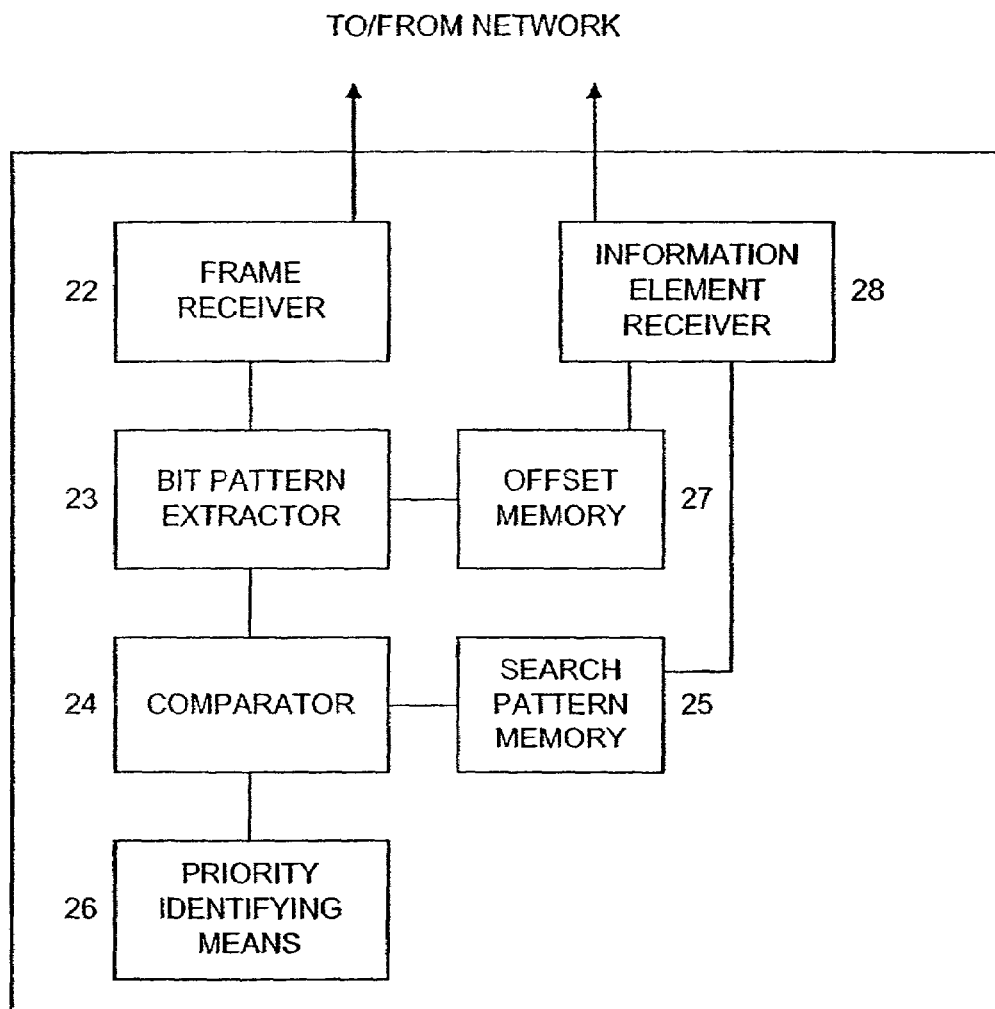


FIG. 3



**FIG. 4**



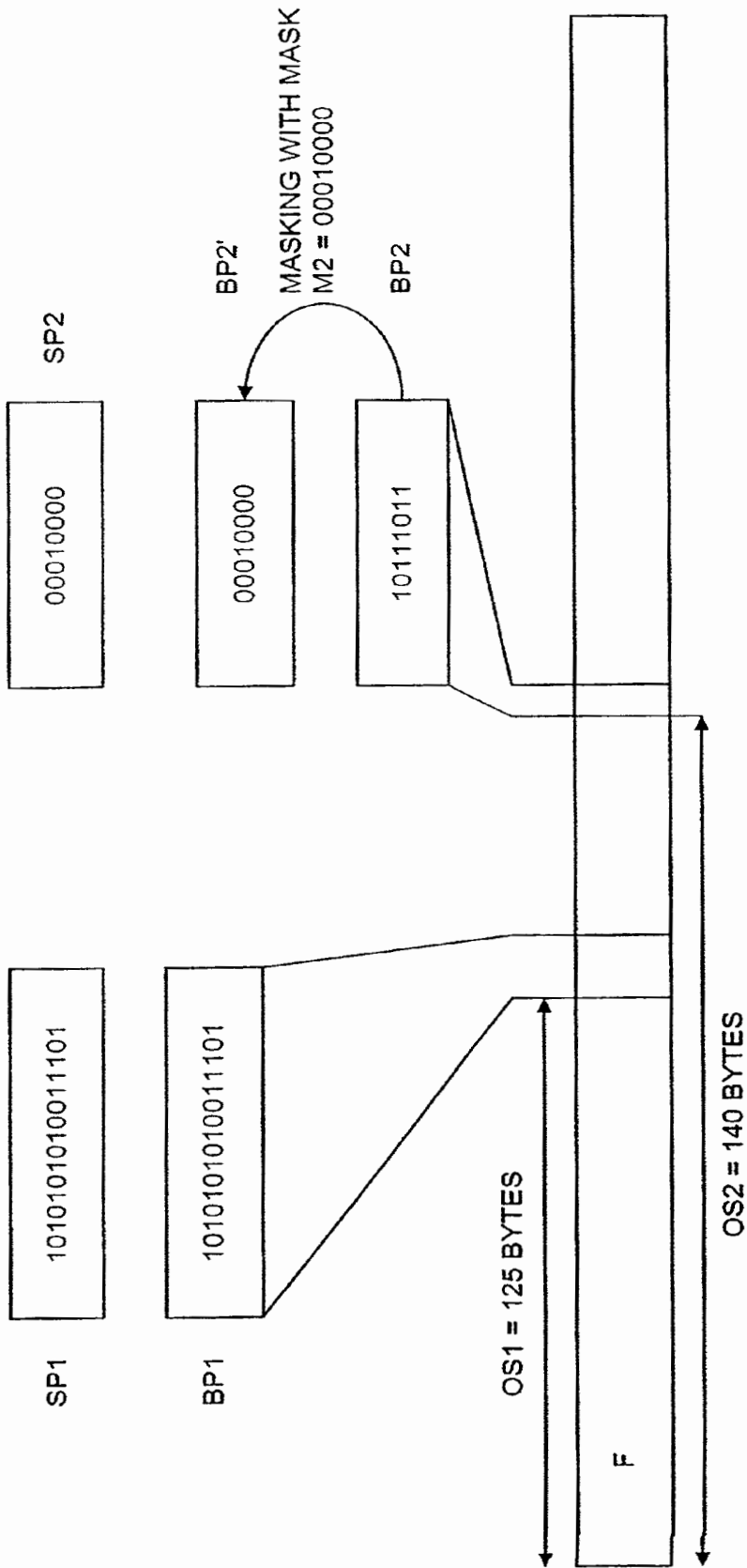


FIG. 5

U.S. Patent

Apr. 11, 2006

Sheet 5 of 10

US 7,027,465 B2

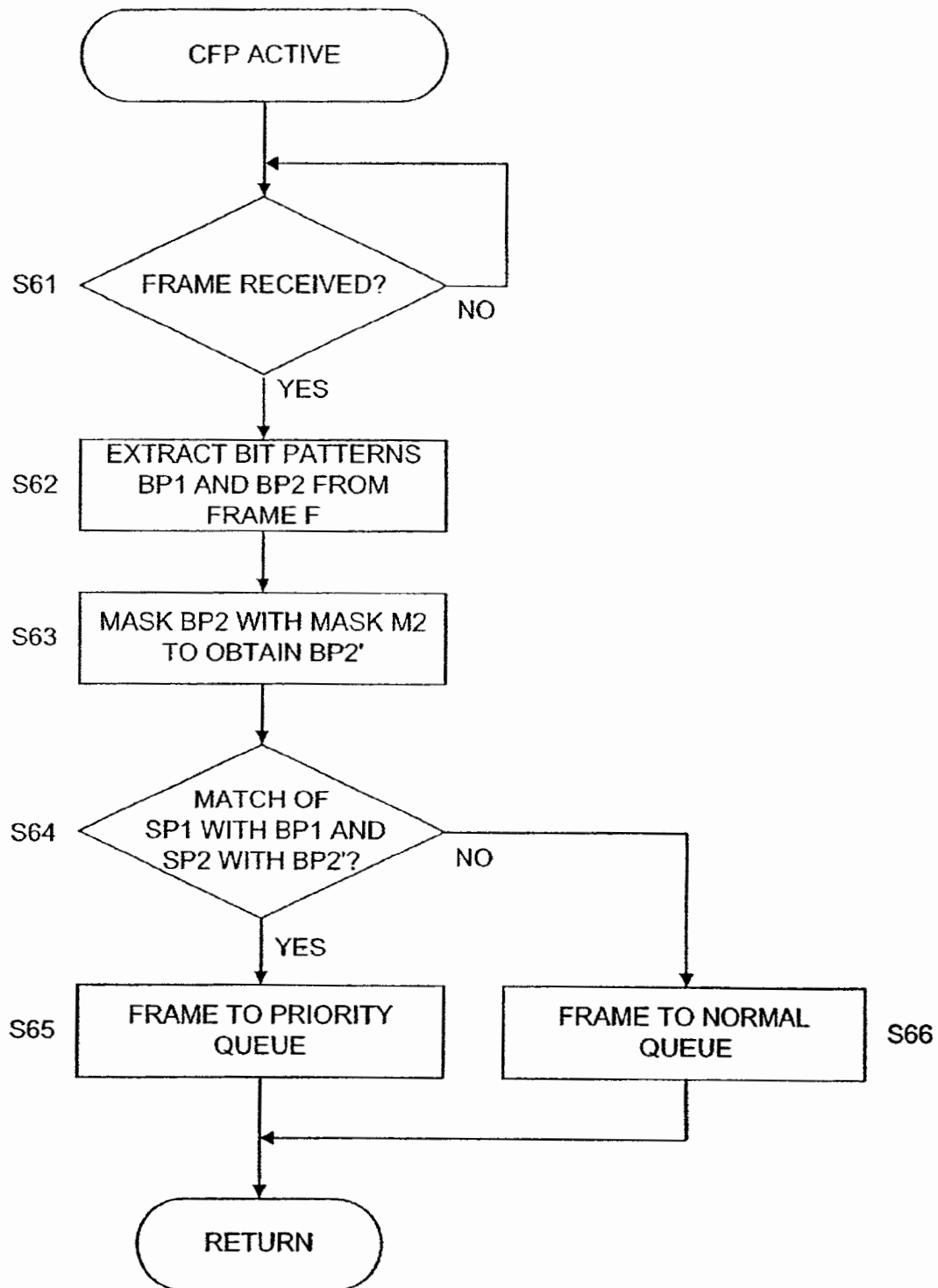


FIG. 6

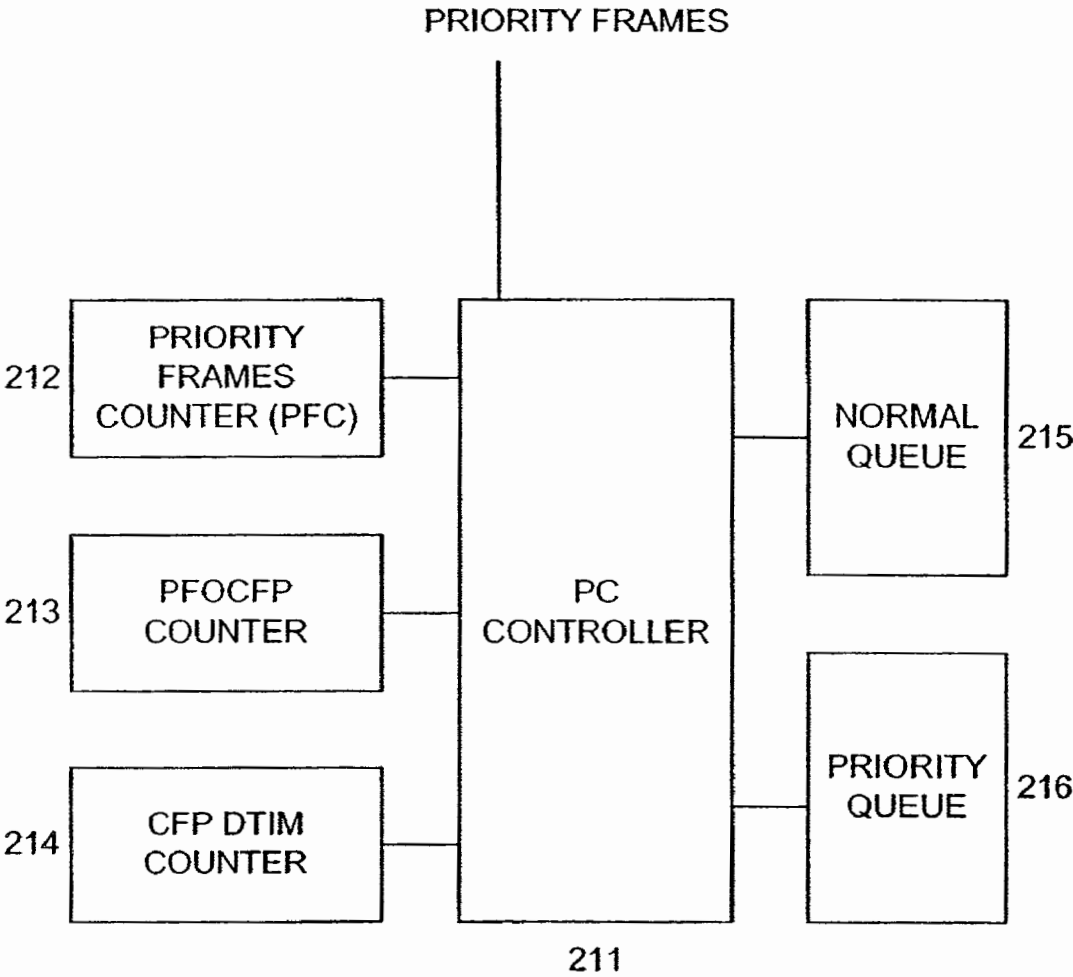


FIG. 7

U.S. Patent

Apr. 11, 2006

Sheet 7 of 10

US 7,027,465 B2

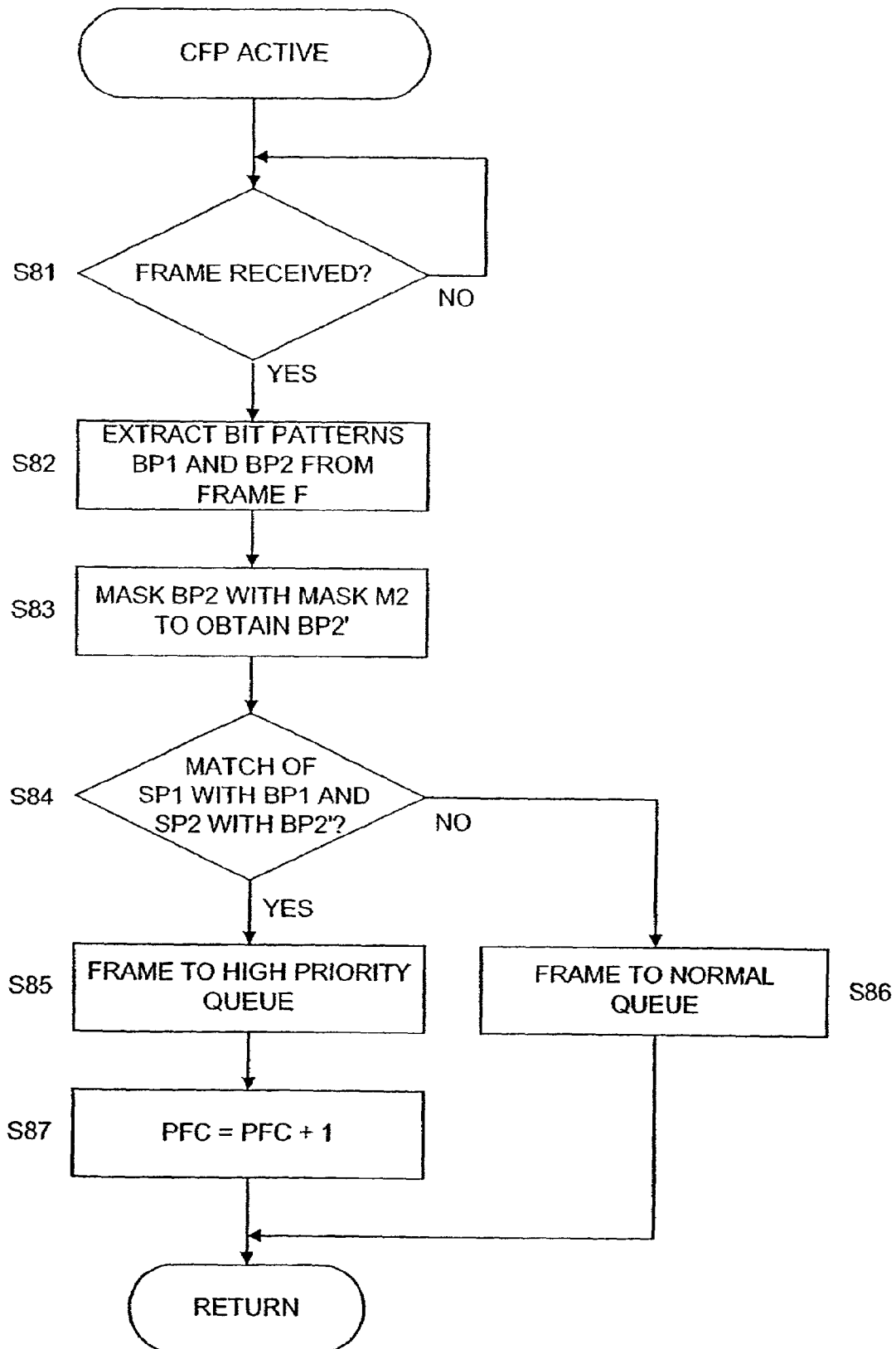


FIG. 8

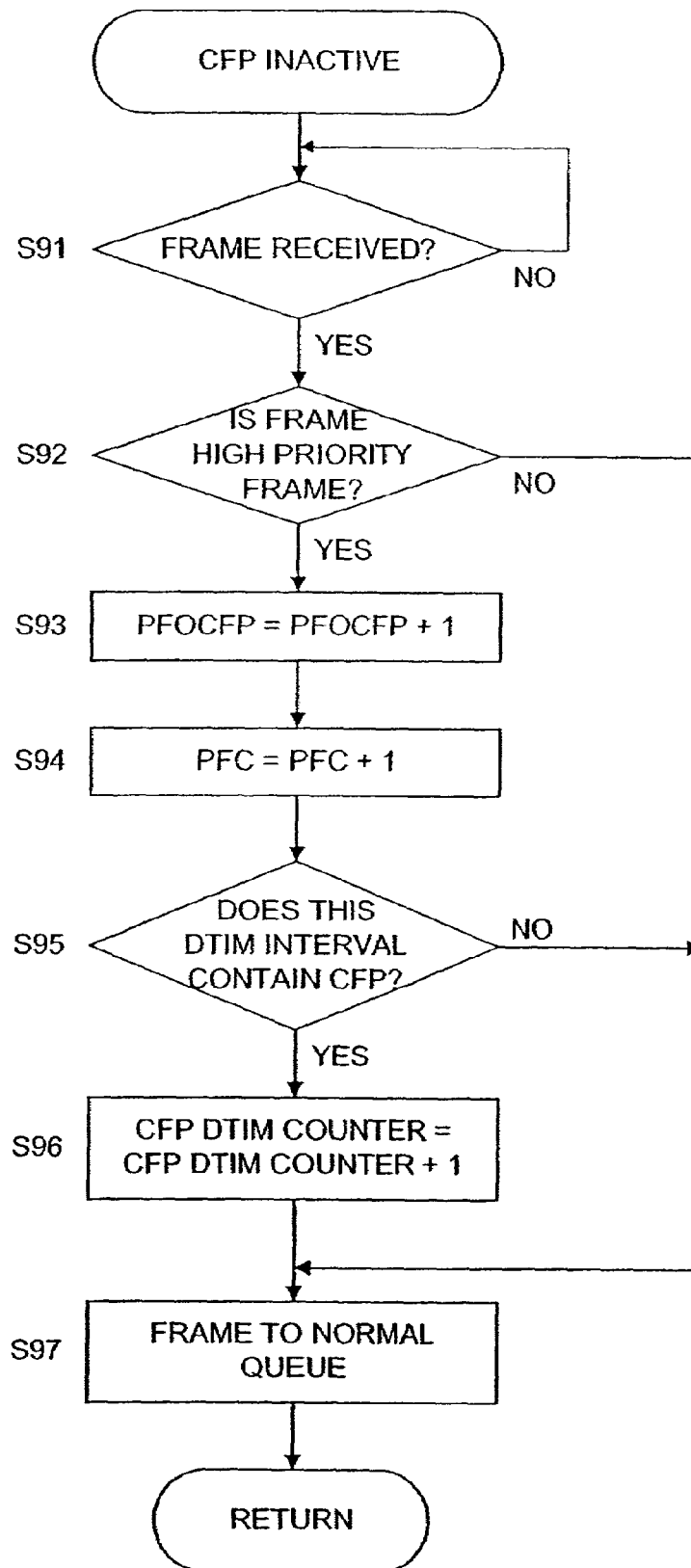


FIG. 9

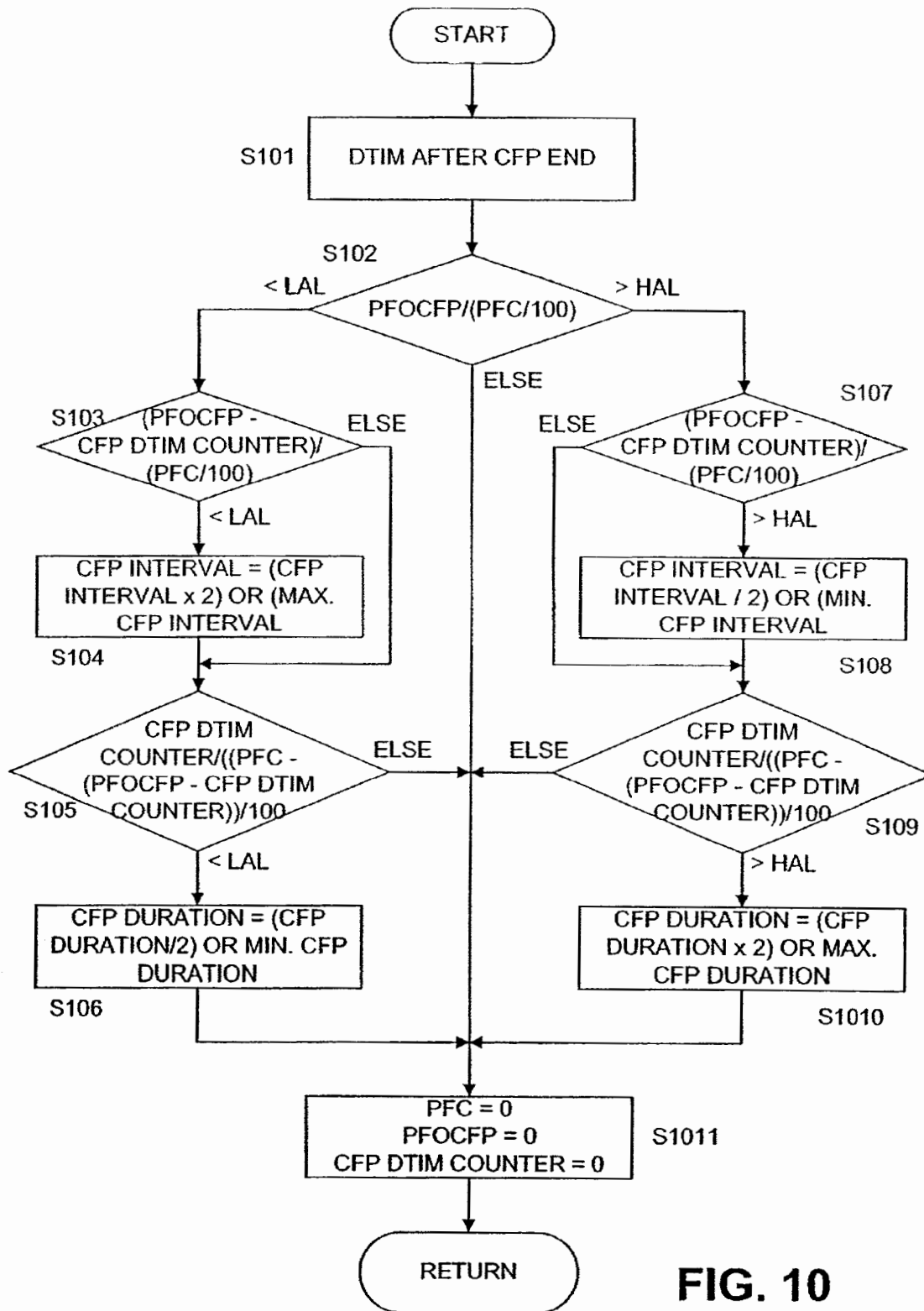


FIG. 10



U.S. Patent

Apr. 11, 2006

Sheet 10 of 10

US 7,027,465 B2

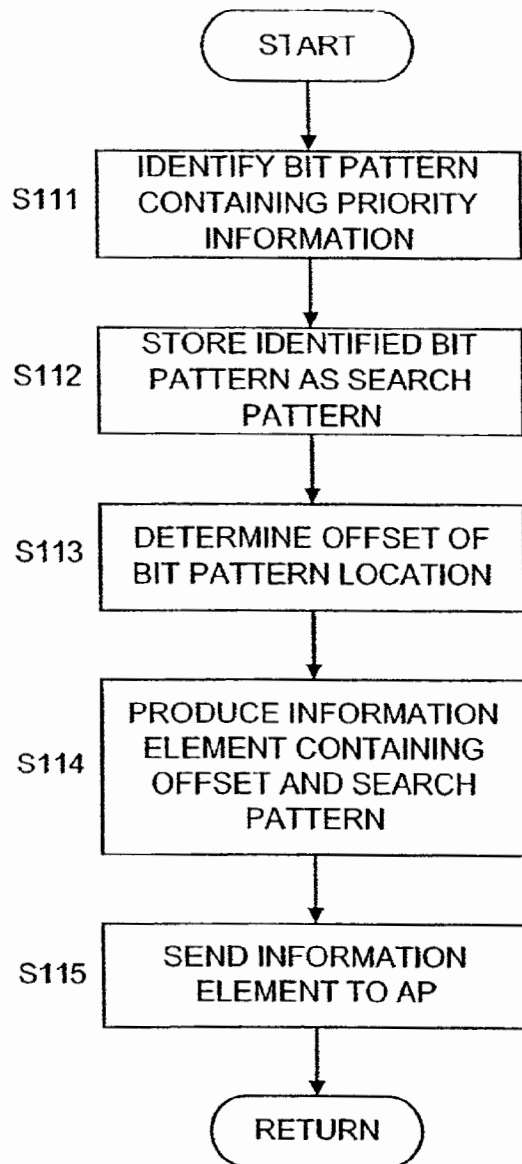


FIG. 11

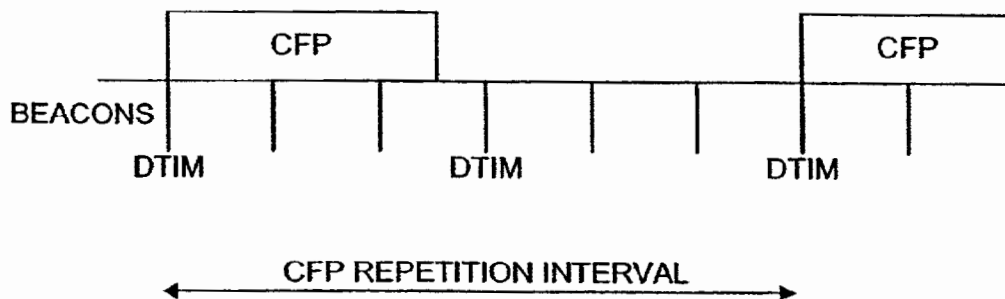


FIG. 12

US 7,027,465 B2

1

**METHOD FOR CONTENTION FREE  
TRAFFIC DETECTION****CROSS-REFERENCE TO RELATED  
APPLICATION**

This application is a continuation of International Application PCT/EP99/10097 having an international filing date of Dec. 17, 1999 and from which priority is claimed under all applicable sections of Title 35 of the United States Code including, but not limited to, Sections 120, 363 and 365(c).

**FIELD OF THE INVENTION**

The present invention relates to a method and a device for detecting priority of data frames in a network.

**BACKGROUND OF THE INVENTION**

This invention relates in general to the field of telecommunications, more precisely to Wireless Local Area Networks (WLAN) and Electrical and Electronics Engineers (IEEE) 802.11 WLAN standard.

The IEEE 802.11 Wireless Local Area Network specification specifies a so-called Contention Free Period (CFP), which is a period of transmission time that is free from the normal contention based airtime reservation. The length and duration of CFP are configurable parameters in Access Point (AP), so that the start of CFP is repeated after one or more Delivery Traffic Indication Message (DTIM) intervals (see IEEE 802.11 standard). The CFP and its relationship to the so-called Content Period (CP) is schematically illustrated in FIG. 12. As can be seen, a CFP repetition interval contains a Content Free Period (CFP) and a Content Period (CP). Each CFP begins with a beacon frame that contains a DTIM element.

The purpose of this CFP is that it can be used for delivering high priority traffic, which has higher real time requirements than normal traffic. The CFP is controlled by the so-called Point Coordination Function (PCF) in an Access Point (AP). The standard specifies the PCF operation in basic level, but does not specify how the PCF should be controlled or how some traffic should be identified as high priority traffic. These things are considered to be out of the scope of the standard.

Information within data frames is marked as having a high priority by using certain fields in some protocol frames or headers. However, the Access Point (AP) usually processes only frames on the Medium Access Control (MAC) layer such that the AP can not easily access information regarding the priority of certain data blocks within the frames, since this information is processed in higher layers.

Thus, for getting priority information, conventionally the frames which are to be transmitted through an Access Point (AP) had to be searched for these fields which indicate the priority state of the actual data frame. This means that in all frames all fields had to be checked, all the headers had to be analyzed, starting from the outer most headers, until the right field in the header had been found.

Since all frame headers are parsed when detecting priority, this measure has a high reliability.

However, this measure is very complex, takes a long time and requires a large amount of processing. Furthermore, the traffic transferred in WLAN can be practically anything, including complex tunneling protocols.

Therefore, all the frame headers and protocols which can be included in the data frames transmitted via the network

2

have to be known. Hence, the amount of information needed for identifying the data is huge. This huge amount of information is typically too heavy to handle in quite small and low price equipment like WLAN access points (AP).

In addition, it has to be considered that every time new protocols are introduced, the access point has to be updated, at least by software updates. This is also required in case protocols already used are changed.

Thus, conventionally such a transmission differentiation based on priority was not conducted at all. That is, the existing systems according to the IEEE 802.11 standard do not separate traffic based on priority. In these conventional systems, the Content Free Period (CFP) is only used to deliver traffic from the Access Point (AP) to stations, treating all frames equally.

**SUMMARY OF THE INVENTION**

Therefore, the object underlying the invention resides in removing the above drawbacks of the prior art and to provide a method by which priority traffic can easily be distinguished from normal traffic without the need of a complex processing.

This object is solved by a method for detecting priority of data frames in a network comprising the steps of extracting a bit pattern from a predetermined position in a frame, comparing the extracted bit pattern with a search pattern, and identifying the received frame as a priority frame in case the extracted bit pattern matches with the first search pattern.

Alternatively, the above object is solved by a device for detecting priority of data frames in a network comprising a receiving means for receiving data frames, an extracting means for extracting a bit pattern from a predetermined position of a data frame, a comparing means for comparing the extracted bit pattern with a predetermined search pattern, and an identifying means for identifying the received frame as a priority frame in case the extracted bit pattern matches with the first search pattern.

Thus, a priority which is defined in a higher-level layer can easily be detected by comparing a corresponding bit pattern with a search pattern without further processing of the received frame. By the method and the device according to the invention, simply a bit pattern is extracted at a position in the frame, where the priority information is known to be located. This bit pattern is compared with a search pattern which corresponds to that bit pattern, which would be located at the above position in case that a priority is set for the actual frame. Thus, it is not necessary to process and analyze the received frame, i.e., to process higher-level layers in order to obtain priority information.

Hence, when adopting the IEEE 802.11 WLAN standard, the priority can be detected in the Medium Access Control (MAC) layer which is a low-level layer. That is, the method can easily find higher priority traffic from the stream of MAC layer frames. Therefore, the method does not need any knowledge of the upper layer protocols.

Consequently, according to the method of the invention, certain traffic can be defined to have higher priority than other traffic when it is handled in an IEEE 802.11 WLAN Access Point (AP). The method is designed so that it is as lightweight as possible to execute in a low cost and possibly low performance AP.

Furthermore, the method is protocol-independent and so flexible that all the configuration may be done in external configuration program and the Access Point does not need to know anything about the processed traffic.

Further advantageous developments are set out below.

US 7,027,465 B2

3

In particular, the predetermined position in the frame is defined by the offset of the bit pattern in the frame. Thus, the position of the bit pattern to be extracted and examined can accurately be defined.

Furthermore, the offset and the search pattern are included in an information element. This information element can be produced by an external program such that the device according to the invention and the device performing the method according to the invention does not have to generate the search pattern and the offset. Thus, the structure of the device does not have to be complex.

In addition, in case new protocols or modified protocols are introduced in the network, it is not necessary to reconfigure the network element (i.e., the device) performing the method. It is only necessary to provide new information elements including the new offset and the new search pattern, which can be effected by an external configuration program. For this, it is not necessary to install new software in the network element or to install new hardware. It is not even necessary to shut down the network element for a new configuration. Hence, the method is very flexible.

Moreover, the bit pattern can be masked by using a mask. Then, the masked bit pattern is compared with the search pattern instead of comparing the bit pattern with the search pattern. By this measure, single bits can easily be extracted from the bit pattern. This is advantageous in case the bit pattern is extracted in form of bytes. For example, a bit pattern can include two bytes, whereas for the priority detection only two bits of each byte are required. These two bits can easily be extracted by using the mask.

The mask can also be included in the information element described above.

If necessary, also a plurality of different bit patterns, search patterns, offsets and—optionally—masks can be used to detect priority of the frames. By this measure, priority information can be detected which is located at different positions within a data frame.

Alternatively, a plurality of different priority levels can be provided for the frames. For detecting different priority levels, a plurality of different bit patterns, search patterns, offsets and—optionally—masks can be used to detect the plurality of different priority levels. By this measure, also different priority levels can easily be detected.

Hence, a plurality of different information elements can be used. For example, one certain priority can require a plurality of information elements, while another certain priority can require only one particular information element.

A received frame can be forwarded to a priority queue in case the frame is detected to be a priority frame during a special period for sending priority traffic. The priority queue serves to transmit the data priority frames in the network faster than normal frames. This measure is especially advantageous in an IEEE 802.11 WLAN since in this standard, a Contention Free Period is defined, as described above.

In addition, the duration of the special period for sending priority traffic can be adjusted according statistical information regarding the priority frames sent. Thus, the special period, i.e., the Contention Free Period, can be adjusted corresponding to the load of priority traffic on the network.

Furthermore, for obtaining the statistical information, the total number of priority frames and the number of priority frames outside the special period can be counted. Then, it can be decided on the basis of the count values obtained whether the special period has to be increased or decreased.

In addition, in the IEEE 802.11, a data+CF-poll frame is defined. Preferably, this data+CF-poll frame can be used for

4

transmitting priority frames in case of a symmetrical high priority traffic between the Access Point and stations in the network.

Furthermore, the invention proposes a method for generating priority detecting information necessary for the above method and device. This method comprises the steps of analyzing a data frame, identifying a bit pattern indicating a priority state, defining the identified bit pattern as a search pattern, and locating the bit pattern within the data frame. By this method, the necessary priority detection information can easily be provided. For example, this method can be employed by a configuration program that is externally run, for example, in one of the wireless stations which are connected by air with the Access Point.

The above method for generating priority detecting information may further comprise the steps of determining the offset of the location, and producing an information element including the offset and the search pattern. Optionally, also the mask for masking the bit pattern mentioned above can be determined and included in the information element.

#### BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

FIG. 1 shows a main system overview;

FIG. 2 shows a process for checking priority of frames according to a first embodiment;

FIG. 3 shows an example for a frame to be examined by the process according to the first embodiment;

FIG. 4 shows a frame priority detecting device according to the first embodiment;

FIG. 5 shows an example of pattern matching with two different information elements according to a second embodiment;

FIG. 6 illustrates a flow chart of a frame sending procedure during Content Free Period (CFP) according to the second embodiment;

FIG. 7 shows relevant parts of a Point Coordinator (PC) according to a third embodiment;

FIG. 8 illustrates a flow chart of a frame sending procedure during Content Free Period (CFP) according to the third embodiment;

FIG. 9 illustrates a flow chart of a frame sending procedure during contention period according to the third embodiment; and

FIG. 10 illustrates a flow chart of a procedure for CFP parameter tuning according to the third embodiment;

FIG. 11 shows a flow chart of a method for obtaining priority detection information; and

FIG. 12 illustrates the relationship between Content Free Periods (CFP) and Content Periods (CP) according to IEEE 802.11.

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following, preferred embodiments of the invention are described in more detail with reference to the accompanying drawings.

FIG. 1 shows an overview of the main system used in the embodiments. The system is a normal IEEE 802.11 Basic Service Set (BSS) containing one Access point (AP) 2 and one or more wireless stations (STA) 3 to 5. The AP may or may not be connected to another wired or wireless network 1. The purpose of the AP 2 is to transmit the traffic between

## US 7,027,465 B2

5

the wireless stations or between wireless stations and the network **1** which is connected to the AP **2**.

All the network components function according to the IEEE 802.11 standard. This presented set-up is a typical representation of the coverage area of one AP. The whole wireless network usually consists of several of these kinds of subsystems. An external configuration program may run in one of the stations in the wireless network or it may reside in some other host and be connected to AP with a wire. In this example, the configuration program is executed in the wireless station **3**.

In the following, a first embodiment which shows the basic idea of the invention is described with respect to the flow chart shown in FIG. **2** and an example for a Medium Access Control (MAC) layer frame shown in FIG. **3**.

The procedure shown in FIG. **2** is executed by the Access Point AP **2** every time a Medium Access Control (MAC) layer frame has been received.

In step S1, the AP **2** extracts a bit pattern from a given position in the received frame. The bit pattern can be a pattern of two bytes, for example. However, the length of the bit pattern can be selected arbitrarily. The extracted bit pattern is indicated by BP in FIG. **2**. In step S2, the extracted bit pattern BP is compared with a predetermined search pattern SP. If in step S3 it is decided that both patterns match, it is determined in step S4 that the actual frame is a priority frame. On the other hand, if it is decided in step S3 that both patterns do not match, it is determined in step S5 that the actual frame is not a priority frame. After identifying the priority of the frame, the frame can be treated according to the identified priority.

Thus, the frame can easily be examined whether it is a priority frame or not without the need for analyzing the data format in the MAC layer frame itself, i.e., without knowing protocols of the higher layers.

The position of the bit pattern to be extracted is defined by the offset OS from the start of the MAC frame, as shown in FIG. **3**. Thus, the AP **2** requires only information regarding the offset OS and the search pattern SP for checking priority of certain MAC frames.

This information can be provided by an external configuration program. The configuration program can be executed in one of the wireless stations, for example. Alternatively, it can be executed in any suitable network element, including the Access Point itself. For this configuration program it is necessary that the bit positions of the priority information which are usually set in higher layers are known. Thus, by providing the AP with the offset, the AP does not have to process the frame in order to identify priority information. It is only necessary to obtain the corresponding bit pattern.

In the first embodiment, the configuration program is executed in the wireless station STA **3**. The configuration program produces information elements which contain the above-described information regarding the offset OS and the search pattern SP necessary to identify the priority state of certain MAC frames. These information elements are transmitted to the AP **2**.

FIG. **4** shows the relevant parts of the Access Point **2** in more detail. Reference numeral **22** denotes a frame receiver by which frames are received from the wired or wireless network **1** and also from the wireless stations **2** to **5**. Reference numeral **23** denotes a bit pattern extractor by which the bit pattern BP described above is extracted from a predetermined position. The position is defined by the offset OS, as mentioned above, and the offset is stored in an offset memory **27** which is accessed by the bit pattern extractor **23**. The extracted bit pattern BP is forwarded to a

6

comparator **24** which compares the extracted bit pattern BP with the search pattern SP. The search pattern SP is stored in a search pattern memory **25** which is accessed by the comparator **24**. The comparison result is supplied to a priority identifying means **26** which identifies the actual frame F as a priority frame in case the comparison results indicates that the bit pattern BP matches the search pattern SP. Thus, the Access Point (AP) **2** can detect priority frames and can treat them correspondingly.

As mentioned above, the external configuration program provides information elements which each comprise an offset OS and a search pattern SP. These information elements are received by an information element receiver **28**. The receiver **28** analyzes the information element and supplies the detected offset OS to the offset memory **27** and the detected search pattern SP to the search pattern memory **25**.

The first embodiment described above illustrates the basic operation according to the invention. The second embodiment described in the following describes a further, more detailed example for the high priority traffic detection method in which the Content Free Period (CFP) defined in IEEE 802.11 standard is used for transmitting detected high priority frames.

According to IEEE 802.11, the Content Free Period (CFP) is a period which is reserved for transmitting high priority traffic, as described above in the introductory part with respect to FIG. **12**. The CFP is controlled by a Point Coordinator (PC) **21** which is arranged in the Access Point (AP) **2** shown in FIG. **1**. If the high priority traffic is transferred only from the AP **1** to the wireless stations (i.e., in a typical client-server application case), the CFP may be used only for delivering data from the AP to wireless stations. But, if the nature of the high priority traffic is interactive (like a videoconference, for example), the PC **21** must also poll wireless stations to permit them to transmit also during the CFP. See IEEE 802.11 standard for more detailed description about this basic functionality of IEEE 802.11 standard.

The AP **2** receives MAC layer frames either from the wireless station or from the connected wired network. If the destination of the frame is in the wireless network, the AP will check whether the frame is high or normal priority traffic. The priority detection requires that the AP **2** is configured with the external configuration program to detect the priority and the required configuration information elements are configured to the AP by the external configuration program. The AP also needs to reformat the MAC level header of the frame or encapsulate the frame inside a separate IEEE 802.11 MAC header which is defined in IEEE 802.11. The point when the priority detection check is performed (before or after IEEE 802.11 MAC header formatting) can be left implementation specific.

If the BSS is in a so-called Contention Free (CF) state (i.e., currently there is a Contention Free Period (CFP)) and the frame is a priority frame, the frame is put in a priority transmit queue, otherwise the frame is treated like the normal traffic. During the CFP, all the frames in the priority queue are transmitted before any frames from the normal queue. When the CFP ends, remaining frames in the priority queue are moved to the normal queue and priority queue is flushed.

According to this embodiment, the priority of a MAC layer frame is detected by using one or more information elements which are transmitted to the Access Point (AP) **1**. That is, one or more bit patterns with corresponding different offsets are checked whether they match with one or more different search patterns. Furthermore, the bit patterns



## US 7,027,465 B2

7

extracted from the MAC layer frame are also masked by using a mask. The mask is also contained in an information element. Thus, the information element according to the second embodiment comprises the offset and the search pattern as according to the first embodiment, and in addition a mask. The mask serves to obtain only particular bits in the extracted bit pattern and is optional.

The operation according to the second embodiment is described by referring to FIGS. 5 and 6. It is noted that for simplifying the illustration, the second embodiment is described with reference to the case that the priority is detected by using two information elements.

In FIG. 5 it is shown that two bit patterns BP1 and BP2 are extracted from the MAC layer frame F. The first bit pattern BP1 is extracted with an offset OS1. As illustrated, the first bit pattern matches with the first search pattern SP1. For the first bit pattern BP1, no mask has been specified (i.e., no masking is performed).

However, for the second bit pattern BP1 a mask M2 is specified. In this example, the mask is M2=00010000 such that only the fourth bit is passed through. The resultant bit pattern BP2' is then compared with the second search pattern SP2. Here, the second search pattern SP2 and the masked bit pattern BP2' match. Since also the first search pattern SP1 matches with the first bit pattern BP1, it is decided that the actual frame F is a high priority frame.

According to the second embodiment, the frame F which has been detected as a priority frame, is transmitted in the Contention Free Period (CFP). That is, it is put on a high priority queue. This process is described in the following by referring to the flow chart shown in FIG. 6.

The process shown in this flow chart is performed during the Content Free Period, i.e., in case the CFP is active. In step S61, the Access Point (AP) 2 waits for receiving a frame which is to be transmitted further to the wireless stations 3 to 5 (FIG. 1). In step S62, the bit patterns BP1 and BP2 are extracted from the frame F, as shown in FIG. 5. In step S63, the bit pattern BP2 is masked with the mask M2 to obtain a bit pattern BP2', as described above. Since no mask has been specified for the first bit pattern BP1, no corresponding step for the first bit pattern BP1 is performed.

Then, in step S64, it is checked whether both bit patterns BP1 and BP2' match with the search patterns SP1 and SP2, respectively. If SP1 and BP1, and SP2 and BP2' respectively match, it is decided that the received frame F is a high priority frame, and the frame F is put in the priority queue (step S65). This is effected by the Point Coordinator (PC) 21 arranged in the Access Point (AP) 2. If the patterns do not match (NO in step S64), the received frame F is put in the normal queue, as shown in step S66.

As described above, the Point Coordinator (PC) 21 puts a priority frame in the priority queue in case the Contention Free Period (CFP) is active. However, in case the CFP is inactive, the frame goes to the normal queue so that it does not have to wait for the CFP to start. When the CFP starts, the PC flushes the normal queue and places the unsent high priority frames in the priority queue. Thus, when the Point Coordinator (PC) 21 notices that the frame which should be sent is a high priority frame, it puts this frame in the normal or high priority queue depending on the current state of the network.

As mentioned above, the use of two information elements is only an example. The number of information elements can be more than two. By using a plurality of information elements, it is also possible to distinguish between different priority levels. For example, the configuration program can give the following data to the Access Point by which three

8

priorities (i.e. priority 1, priority 2 and priority 3) can be distinguished. It is noted that these three priorities can each represent different priority levels (e.g., priority 1 represents the highest priority while priority 3 has the lowest) or can represent equal priority levels.

Priority 1 Information:

Information element 1: offset 1 and search pattern 1

Information element 2: offset 2 and search pattern 2

Information element 3: offset 3 and search pattern 3

...

Information element n: offset n and search pattern n

Priority 2 Information:

Information element 1: offset 1 and search pattern 1

Priority 3 Information:

Information element 1: offset 1 and search pattern 1

Information element 2: offset 2 and search pattern 2

The AP then checks whether a received frame matches with all the information elements of the first group containing the information elements for priority 1. That is, for each information element it is checked whether a bit pattern at the offset included in the information element matches with the search pattern included in the information element. If this is the case for all information elements, then the frame has the priority 1.

If the frame does not match with all information elements listed in the first group, then the AP tests the same frame with all the information elements (one, in this example) of the second group containing the information elements for priority 2. If the bit pattern extracted at the offset 3 in the frame matches with the search pattern 3 included in information element 3, it is decided that the frame has the priority 2.

However, if the patterns do not match, then the AP checks the priority 3 information. That is, the frame is checked whether it matches with information elements 1 and 2. If this is the case, the frame has the priority 3. If the frame still does not match, it has no priority.

Next, a third embodiment is described, according to which the Point Coordinator (PC) 21 collects statistics about the high priority traffic sent and adjusts the parameters for the CFP.

In detail, the PC 21 counts the high priority packets during the every so-called Delivery Traffic Indication Message (DTIM) interval (see IEEE 802.11 WLAN standard). Furthermore, it also counts how much of those packets are transmitted outside the CFP and how much during the DTIM interval containing CFP but outside CFP. The PC saves statistics of the previous N DTIM intervals, where N is at least the CFP repeating interval. The PC then checks the statistics after every DTIM interval that contains CFP and adjusts the CFP length and interval accordingly. The frame handling and statistics collection during the CFP is presented in FIG. 8 and during the contention period in FIG. 9.

The PC 21 according to the third embodiment is shown in FIG. 7 in greater detail. As derivable therefrom, the PC comprises a plurality of counters which are used by a PC controller 211 to control the CFP. A priority frames counter (PFC) 212 serves to count all priority frames received. A counter for priority frames outside CFP (PFOCFP) counter 213 serves to count all priority frames which are received during the content period, i.e., when CFP is inactive. A CFP DTIM counter 214 serves to count all priority frames which are received in an DTIM interval containing a Contention Free Period (CFP). As mentioned above, the PC 21 forwards the received priority frames either to the normal queue 215 or to the priority queue 216 depending on the current state of the network.

## US 7,027,465 B2

9

The flowchart shown in FIG. 8 is almost the same as in FIG. 6. The steps S81 to S86 correspond to the steps S61 to S66 of FIG. 5. Thus, an unnecessary repetition is omitted here. However, in addition to the flow chart shown in FIG. 6, a new step S87 is performed in case patterns SP1 and BP1, and SP2 and BP2' match. In this step S8, the priority frame counter (PFC) 212 is incremented each time it is decided that an actual frame is a high priority frame.

FIG. 9 shows a flowchart representing a process performed during the content period, i.e., when the CFP is inactive. Here, all received frames are put in the normal queue. In case of a high priority frame, several values are counted by the counters of the Point Coordinator (PC) 21 for providing statistical information.

In detail, in step S91 it is waited for a frame, similar to step S81 of FIG. 8. In step S92, the priority is detected in the way as described in the first or second embodiment. If the actual frame is a normal frame with no priority, the flow advances to step S97 in which the frame is put to the normal queue 215. If, however, the actual frame is a priority frame, the flow advances to step S93 in which PFOCFP counter 213 is incremented. Furthermore, in step S94 also the priority frames counter 212 is incremented.

In step S95 it is checked whether the actual DTIM interval contains a Content Free Period (CFP). If this DTIM interval contains a CFP, the CFP DTIM counter 214 is incremented in step S96 before the flow advances to step S97. Otherwise, the flow advances directly to step S97. Thereafter, the routine is ended.

The statistical information regarding the priority frames are used as described in the following with reference to FIG. 10.

As shown in FIG. 10, the procedure is started in an DTIM interval after the end of the Content Free Period (step S101). In step S102, the percentage of priority frames sent outside of the CFP is checked. Depending on the result, different processes are executed, as described next.

If the percentage of high priority traffic sent outside of CFP is higher than a certain high alarm level HAL, the PC 21 will start corrective actions. These processes are illustrated on the right side of the flow chart shown in FIG. 10.

The alarm level is 100%—percentage of the high priority traffic that must be sent inside the CFP in any case. For example, if it is known that the traffic which requires an almost real-time treatment requires a priority traffic of 30%, the alarm level is set to 70%. The alarm level can be fixed or it can be dynamically adjustable.

When the alarm level HAL is reached, the PC will next check the percentage of high priority traffic sent during the DTIM intervals not containing the CFP. This is effected in step S107 in which the difference between the count values of the PFOCFP counter 213 and the CFP DTIM counter 214 is calculated, wherein the difference is brought in relation to the value of the priority frames counter (PFC) 212. If it is more than the alarm level HAL, the PC will make the CFP interval to be half of the original (if it is not already one DTIM interval), as described in step S108.

Next, in step S109, the PC 21 will check if the percentage of high priority traffic sent outside of the CFP during the DTIM intervals containing CFP is also higher than the alarm level. This percentage P is calculated as follows:

$$CFP\ DTIM\ counter / (PFC - (PFOCFP - CFP\ DTIM\ counter)) / 100$$

If this percentage is higher than the alarm level, the PC 21 will double the duration of the CFP (if not already maximum

10

possible) in step S1010. The alarm level used in the different steps may be the same or different according to the wanted system behavior.

If it is decided in step S102 that the percentage of high priority traffic sent outside the CFP drops below a low alarm level LAL, the PC 21 will start decreasing the CFP in order to give the normal traffic also a reasonable chance to be delivered in time. The low alarm level LAL is the percentage of the high priority traffic that can be sent outside the CFP if needed. In order that the system can work smoothly, the low alarm level should be less than 100%—high alarm level HAL.

When the alarm level LAL is reached, the PC 21 will next check what is the percentage of high priority traffic sent during the DTIM intervals not containing the CFP in step S103 which corresponds to step S107 described above. If it is less than alarm level, the PC will make the CFP interval to be double of the original in step S104. Next, the PC 21 will check if the percentage of high priority traffic sent outside of the CFP during the DTIM containing CFP is also lower than the alarm level LAL. This is effected in step S105 which corresponds to step S109 described above. If this percentage is lower as the alarm level LAL, the PC 21 decreases the duration of the CFP with the amount of the previous addition in step S106. The alarm level LAL used in the different steps may be the same or different according to the wanted system behavior.

If it is decided in step S102 that the percentage of priority frames outside the Content Free Period (i.e., the count value of the PFOCFP counter 213 with respect to the count value of the priority frame counter 212) is between the low alarm level LAL and the high alarm level HAL, the flow advances directly to step S1011 in which all counters 212, 213 and 214 are reset. Then, the procedure is ended.

Next, a fourth embodiment is described. The structure and procedures according to this embodiment is similar to the embodiments described above. However, in this embodiment the nature of the high priority traffic is checked. In particular, it is considered whether the high priority traffic is symmetrical, i.e., whether the high priority traffic from a wireless station to the Access Point (AP) 2 is the same or almost the same as the high priority traffic from the AP 2 to the wireless station.

During the Content Free Period (CFP) the wireless stations (terminals) are not allowed to transmit unless the PC 21 polls them. Therefore, they will register themselves to PC to be placed in a polling list. In order to get the best benefit from this traffic control, wireless stations in the WLAN must be able to identify the high priority traffic and send that traffic during the CFP.

In case of the symmetrical high priority traffic between the AP 2 and the wireless stations, the configuration information (from the external configuration program) contains a field telling that this is symmetrical high priority traffic. When the Point Coordinator (PC) 21 in the AP 2 detects that the high priority traffic is symmetrical and the receiving station is pollable during the Content Free Period (i.e., is CF-pollable), it will send it to the terminal inside a so-called data+CF-poll frame instead of normal data frame during the CFP. The data+CF-poll frame is a special data frame, defined in the IEEE 802.11 standard, that allows the receiving station send one data frame during the CFP after receiving the data+CF-poll frame. During the contention period, the symmetrical traffic does not cause any special processes. The use of data+CF-poll frame enables equal high priority data delivering performance to both directions.



US 7,027,465 B2

## 11

The PC 21 must ensure that other wireless stations in the polling list gets polled according to the standard even when delivering symmetrical high priority traffic.

In the following, the configuration program used for generating priority detection information used in the above embodiments is described in more detail.

The method adopted in the configuration program is described by referring to the flowchart shown in FIG. 11.

In step S111, a bit pattern (consisting, for example, of one or two bytes) which indicates the priority information is identified in the data frame. The identified bit pattern is defined as the search pattern (SP) in step S112. In step S113, the location, that is, the offset of the identified bit pattern (i.e., the search pattern) inside the data frame is determined. Thereafter, an information element containing the determined offset and the identified search pattern is produced in step S114. Finally, in step S115 the information element is sent to the Access Point and the routine ends.

In a similar way, also the optional mask (as used in the second embodiment) can be obtained. Therefore, an additional step is required which is performed after the bit pattern identifying step S112 such that the mask is defined. It is also possible to produce a plurality of information elements, as used in the second and third embodiment, also by taking into account a plurality of different priority levels.

Next, an example is described in which frames (containing IP packets) to be sent to a particular IP-address should have high priority. In this case, the identification of the search patterns and the location of the search patterns can be performed as follows: The configuration program knows that the offset to the destination IP-address from the beginning of the IP packet (as an example for a data frame) is 32 bytes and the offset from the beginning of the ethernet (version 2) frame to beginning of the IP packet is 14 bytes. Thus, the actual offset of the IP-address is 46 bytes. The search pattern is the IP-address in question. Thus, the necessary information for an information element can easily be extracted.

In other cases, it might be necessary that the configuration program analyzes frames in order to obtain the relevant information.

The location for performing the above method within the network can be arbitrarily chosen. It may be located in some station in the wireless network, it may be centralized in a place in the wired network, or it may be connected to the AP with a separate cable. In some cases, the configuration program may also be run in the AP, but in this way the benefit of the configuration program being external will be lost.

Preferably, the location where the above method, i.e., the external configuration program can be performed is in one of the wireless stations 2 to 5. In this way, the program can also "snoop" the traffic and check whether the traffic is correctly recognized by the AP, that is, whether the high priority traffic is correctly treated. This is because in the wireless stations, the data sent with the frames are processed and, thus, it is clear whether a received frame is a priority frame or not.

When placed in the WLAN, the configuration program can also make corrections to the AP configurations (i.e., the information elements sent to the AP) based on a traffic monitoring in the WLAN. The configuration program can be run in some notebook PC in WLAN, for example.

In rather large networks, however, the best place for the configuration program is in the wired network, where all the access points of the network can be controlled with a single configuration program.

## 12

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiments of the invention may vary within the scope of the attached claims. For example, the embodiments can be arbitrarily combined.

In particular it has to be noted that the above description of the embodiment has been made basically with respect to the IEEE 802.11 WLAN standard. However, it has to be noted that this is only an example and that it is to be understood that the invention can also be applied to other suitable network situations.

Furthermore, in the above embodiments it was basically distinguished between priority frames and normal frames, i.e., between frames with priority and frames without priority. However, it is also possible to distinguish between a plurality of different priority levels. For example, the second embodiment can be modified such that the two bit patterns are used to distinguish between three different priority levels (no priority—medium priority—high priority). Also, different masks for one bit pattern can be used to distinguish between different priority levels.

The invention claimed is:

1. A method for detecting priority of data frames in a network comprising the steps of
  - extracting a bit pattern from a predetermined position in a frame,
  - comparing said extracted bit pattern with a search pattern, and
  - identifying a received frame as a priority frame in case said extracted bit pattern matches with said search pattern, wherein said predetermined position in said frame is defined by the offset of said bit pattern in said frame.
2. The method according to claim 1, wherein said offset and said search pattern are included in an information element.
3. The method according to claim 1, further comprising the step of
  - masking said bit pattern by using a mask and comparing the masked bit pattern with said search pattern instead of comparing said bit pattern with said search pattern.
4. The method according to claim 3, wherein said predetermined position in said frame is defined by the offset of said bit pattern in said frame, and said offset, said search pattern and said mask are included in an information element.
5. The method according to claim 1, wherein a plurality of different priority levels are provided and a plurality of different bit patterns, search patterns and offsets are used to detect said plurality of different priority levels.
6. A method for detecting priority of data frames in a network comprising the steps of
  - extracting a bit pattern from a predetermined position in a frame,
  - comparing said extracted bit pattern with a search pattern, and
  - identifying a received frame as a priority frame in case said extracted bit pattern matches with said search pattern, wherein a plurality of different bit patterns, search patterns and offsets are used to detect priority of said frames.
7. A method for detecting priority of data frames in a network comprising the steps of
  - extracting a bit pattern from a predetermined position in a frame,
  - comparing said extracted bit pattern with a search pattern,

US 7,027,465 B2

13

identifying a received frame as a priority frame in case  
said extracted bit pattern matches with said search  
pattern, and  
forwarding said received frame to a high priority queue in  
case said frame is detected to be a high priority frame 5  
during a special period for sending priority traffic.  
8. The method according to claim 7, further comprising  
the step of  
adjusting the duration of the special period for sending  
priority traffic according statistic information regarding 10  
sent priority frames.  
9. The method according to claim 8, further comprising  
the steps of  
counting the total number of priority frames;  
counting the number of priority frames outside said 15  
special period; and  
deciding whether said special period has to be increased  
or decreased on the basis of the count values obtained  
in said counting steps.  
10. A device for detecting priority of data frames com- 20  
prising  
a receiving means for receiving data frames;  
an extracting means for extracting a bit pattern from a  
predetermined position of a data frame;  
a comparing means for comparing said extracted bit 25  
pattern with a predetermined search pattern; and  
an identifying means for identifying said received frame  
as a priority frame in case said extracted bit pattern  
matches with said first search pattern, wherein said  
predetermined position is defined by an offset, and 30  
wherein said offset and said search pattern are included  
in an information element.  
11. The device according to claim 10, further comprising  
a masking means for masking said bit pattern by using a  
mask, wherein said comparing means compares the masked 35  
bit pattern with said search pattern instead of comparing said  
bit pattern with said search pattern.  
12. The device according to claim 11, wherein said  
predetermined position in said frame is defined by the offset  
of said bit pattern in said frame, and said offset, said search 40  
pattern and said mask are included in an information ele-  
ment.  
13. The device according to claim 10, wherein a plurality  
of different priority levels are provided and a plurality of  
different bit patterns, search patterns and offsets are used to 45  
detect said plurality of different priority levels.  
14. A device for detecting priority of data frames com-  
prising

14

a receiving means for receiving data frames;  
an extracting means for extracting a bit pattern from a  
predetermined position of a data frame;  
a comparing means for comparing said extracted bit  
pattern with a predetermined search pattern; and  
an identifying means for identifying said received frame  
as a priority frame in case said extracted bit pattern  
matches with said first search pattern, wherein a plu-  
rality of different bit patterns, search patterns and  
offsets are used to detect priority of said frames.  
15. A device for detecting priority of data frames com-  
prising  
a receiving means for receiving data frames;  
an extracting means for extracting a bit pattern from a  
predetermined position of a data frame;  
a comparing means for comparing said extracted bit  
pattern with a predetermined search pattern; and  
an identifying means for identifying said received frame  
as a priority frame in case said extracted bit pattern  
matches with said first search pattern, wherein a con-  
trolling means forwards said received frame to a high  
priority queue in case said frame is detected to be a high  
priority frame during a special period for sending  
priority traffic.  
16. The device according to claim 15, wherein said  
controlling means adjusts the duration of the special period  
for sending priority traffic according statistic information  
regarding sent priority frames.  
17. The device according to claim 16, wherein said  
controlling means, in order to obtain said statistic informa-  
tion, accesses to a priority frames counter for counting the  
total number of priority frames and a counter for counting  
priority frames outside said special period, said controlling  
means deciding whether said special period has to be  
increased or decreased on the basis of the count values  
obtained in said counting steps.  
18. Method for generating priority detecting information,  
comprising the steps of:  
identifying a bit pattern indicating a priority state in a data  
frame,  
defining said identified bit pattern as a search pattern,  
locating said bit pattern within said data frame,  
determining the offset of the location of said bit pattern,  
and  
producing an information element including said offset  
and said search pattern.

\* \* \* \* \*

# Exhibit K

---



US00RE44904E

(19) **United States**  
 (12) **Reissued Patent**  
**Karhula**

(10) **Patent Number:** **US RE44,904 E**  
 (45) **Date of Reissued Patent:** **May 20, 2014**

(54) **METHOD FOR CONTENTION FREE TRAFFIC DETECTION**

(75) Inventor: **Petri Karhula**, Tampere (FI)

(73) Assignee: **Calton Research L.L.C.**, Wilmington, DE (US)

(21) Appl. No.: **13/171,882**

(22) Filed: **Jun. 29, 2011**

#### Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **7,555,014**  
 Issued: **Jun. 30, 2009**  
 Appl. No.: **11/402,621**  
 Filed: **Apr. 11, 2006**

U.S. Applications:

(63) Continuation of application No. 10/167,986, filed on Jun. 11, 2002, now Pat. No. 7,027,465, which is a continuation of application No. PCT/EP99/10097, filed on Dec. 17, 1999.

(51) **Int. Cl.**  
**H04J 3/07** (2006.01)

(52) **U.S. Cl.**  
 USPC ..... **370/506; 370/350**

(58) **Field of Classification Search**  
 USPC ..... **370/350, 503-506**  
 See application file for complete search history.

(56) **References Cited**

#### U.S. PATENT DOCUMENTS

4,627,051 A 12/1986 Shimizu  
 4,716,407 A 12/1987 Borrás et al.  
 4,930,124 A 5/1990 de Boisseron et al.  
 5,541,919 A \* 7/1996 Yong et al. .... 370/416  
 5,594,738 A 1/1997 Crisler et al.

5,675,617 A 10/1997 Quirk et al.  
 5,678,188 A 10/1997 Hisamura  
 5,682,386 A \* 10/1997 Arimilli et al. .... 370/468  
 5,822,361 A 10/1998 Nakamura et al.  
 5,857,092 A 1/1999 Nakamura et al.  
 5,881,242 A 3/1999 Ku et al.  
 6,347,087 B1 \* 2/2002 Ganesh et al. .... 370/392  
 6,633,564 B1 \* 10/2003 Steer et al. .... 370/389  
 6,658,363 B2 12/2003 Mejia et al.  
 7,027,465 B2 4/2006 Hautala

#### FOREIGN PATENT DOCUMENTS

EP 0491494 6/1992  
 EP 0584667 3/1994  
 EP 0749254 12/1996

(Continued)

#### OTHER PUBLICATIONS

R.O. Lamaire et al.; "Wireless LANs and Mobile Networking: Standards and Future Directions"; IEEE communications Magazine 'Online!'; Aug. 1996; p. 1-15.

(Continued)

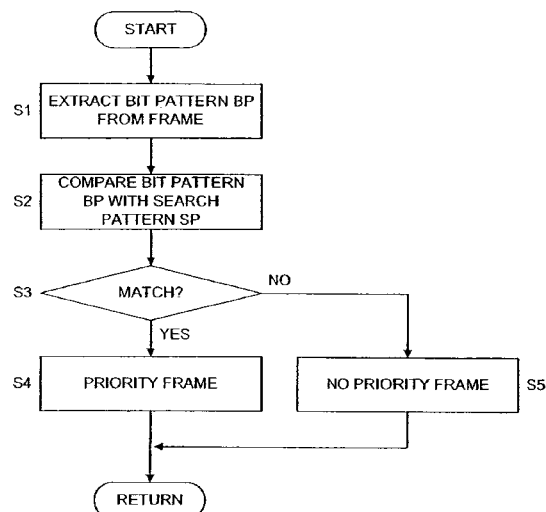
*Primary Examiner* — Phuc Tran

(74) *Attorney, Agent, or Firm* — Stolowitz Ford Cowger LLP

(57) **ABSTRACT**

The invention discloses a method for detecting priority of data frames comprising the steps of extracting (S1) a bit pattern from a predetermined position in a frame, comparing (S2, S3) said extracted bit pattern with a search pattern, and identifying (S4) said received frame as a priority frame in case said extracted bit pattern (BP) matches with said first search pattern (SP). By this method, the priority of a data frame can easily be detected. The invention also proposes a corresponding device for detecting priority of data frames.

**18 Claims, 10 Drawing Sheets**



**US RE44,904 E**

Page 2

---

(56)

**References Cited**

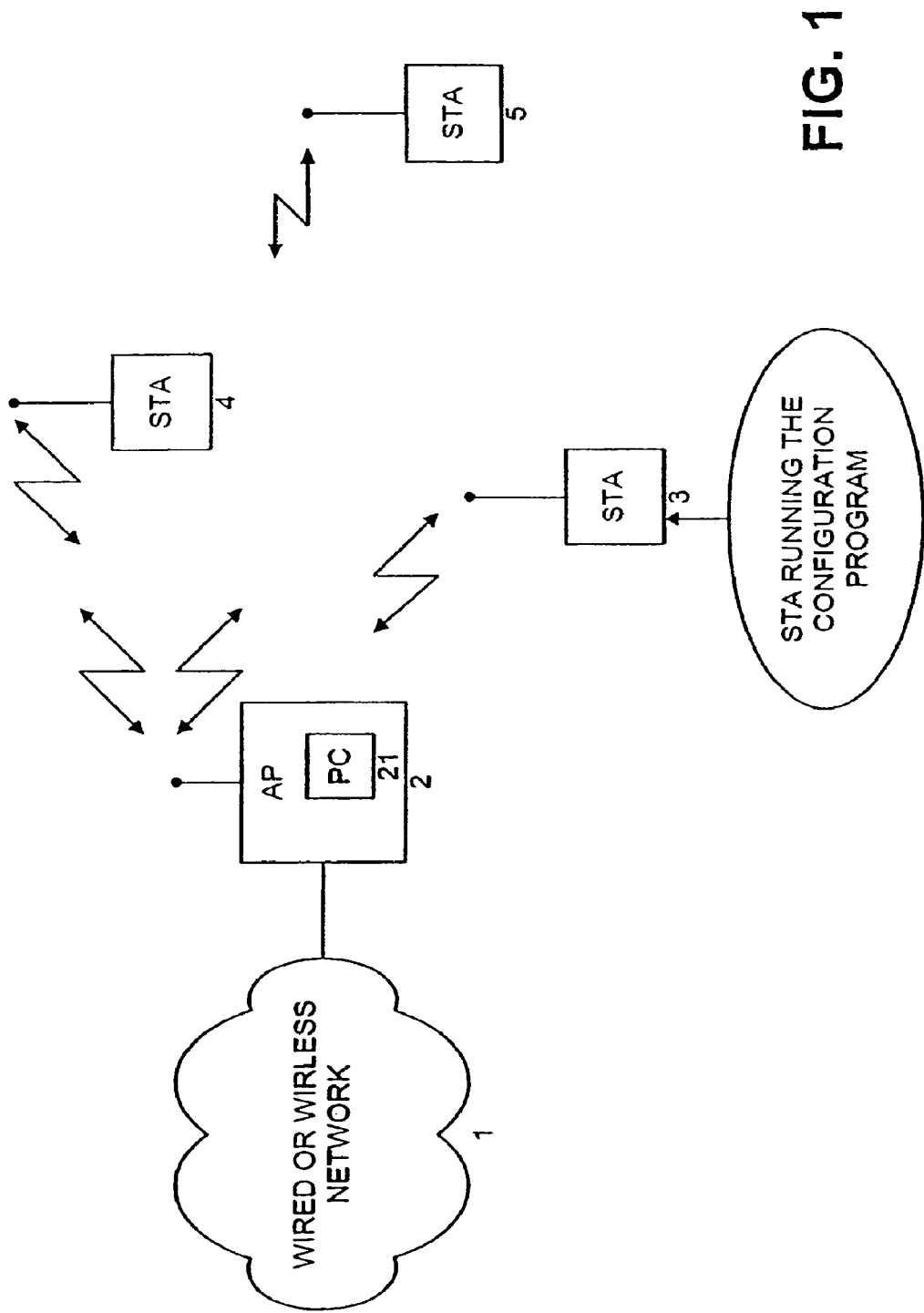
**OTHER PUBLICATIONS**

**FOREIGN PATENT DOCUMENTS**

EP	0782297	7/1997
EP	0804006	10/1997
EP	0917317	5/1999
EP	0959398	11/1999
WO	01045328	6/2001

European Patent Office; International Search Report WO01045328; Apr. 4, 2001; 7 pages.  
Stolowitz Ford Cowger LLP; Related Case Listing; Aug. 24, 2011, 1 Page.

\* cited by examiner





U.S. Patent

May 20, 2014

Sheet 2 of 10

US RE44,904 E

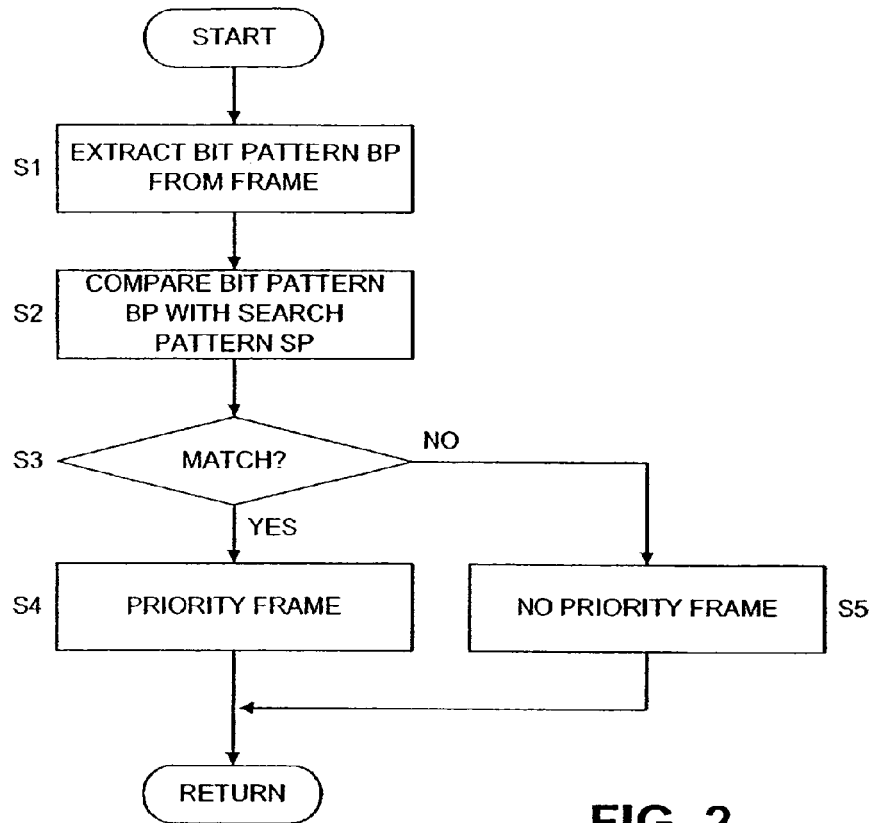


FIG. 2

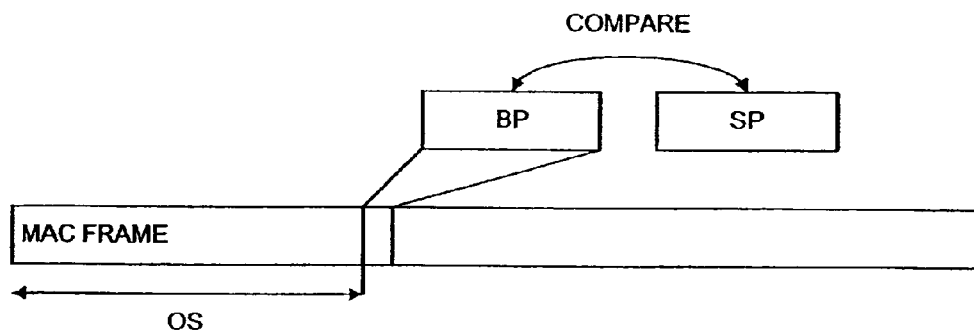
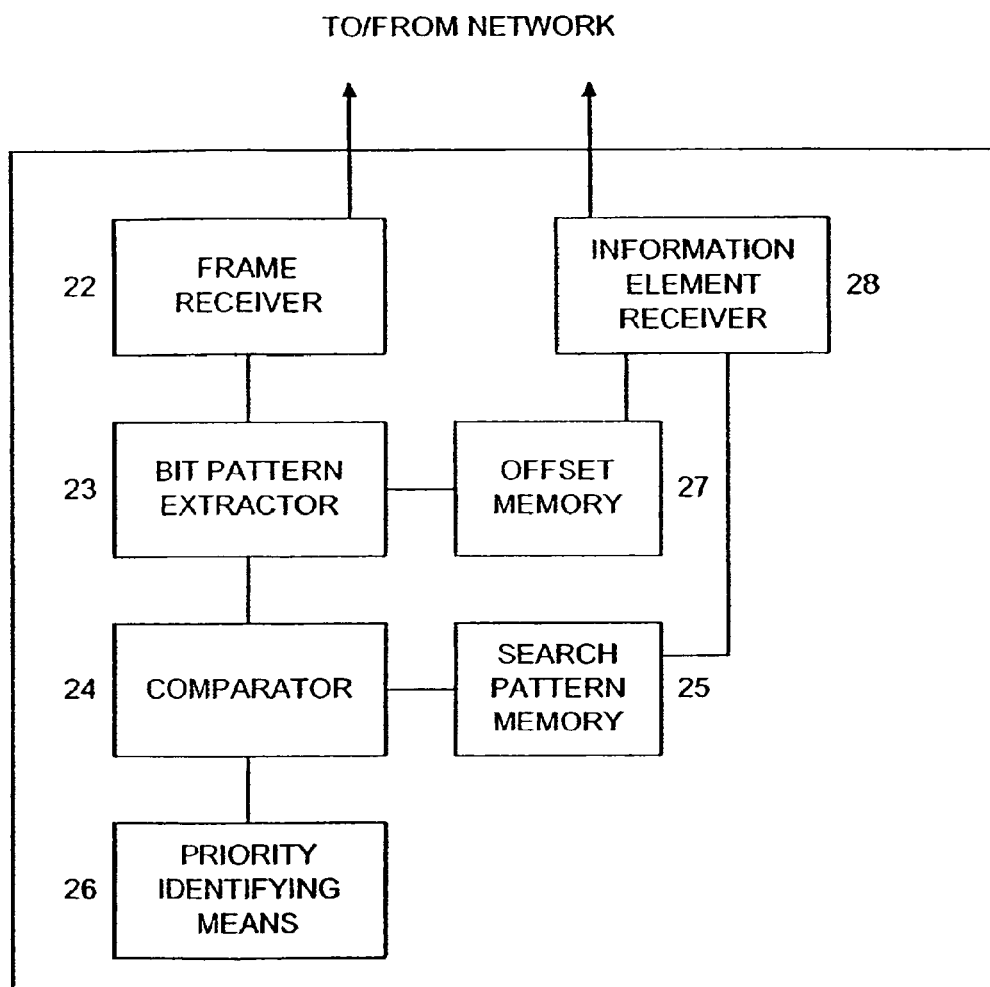


FIG. 3



**FIG. 4**

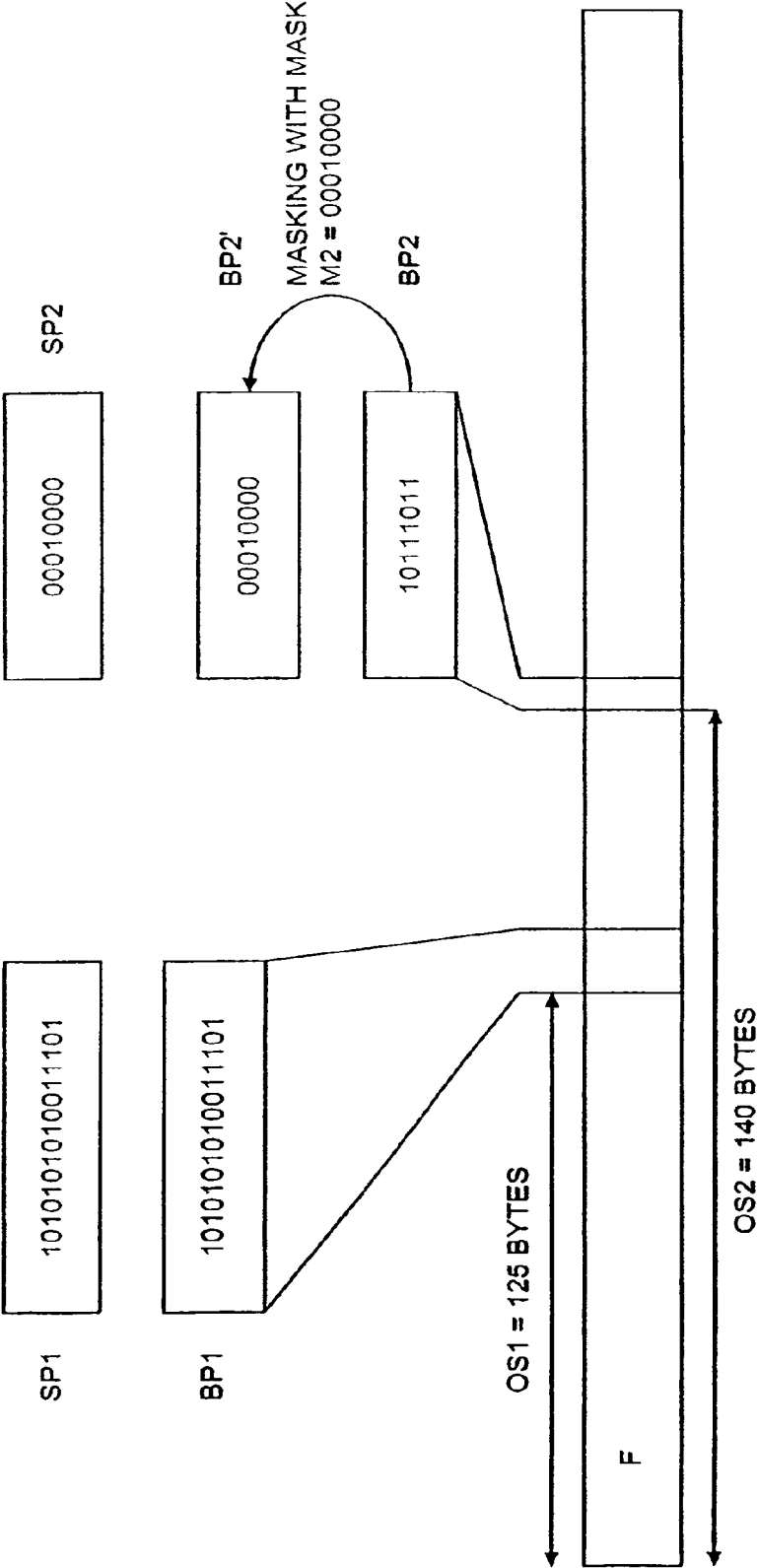


FIG. 5

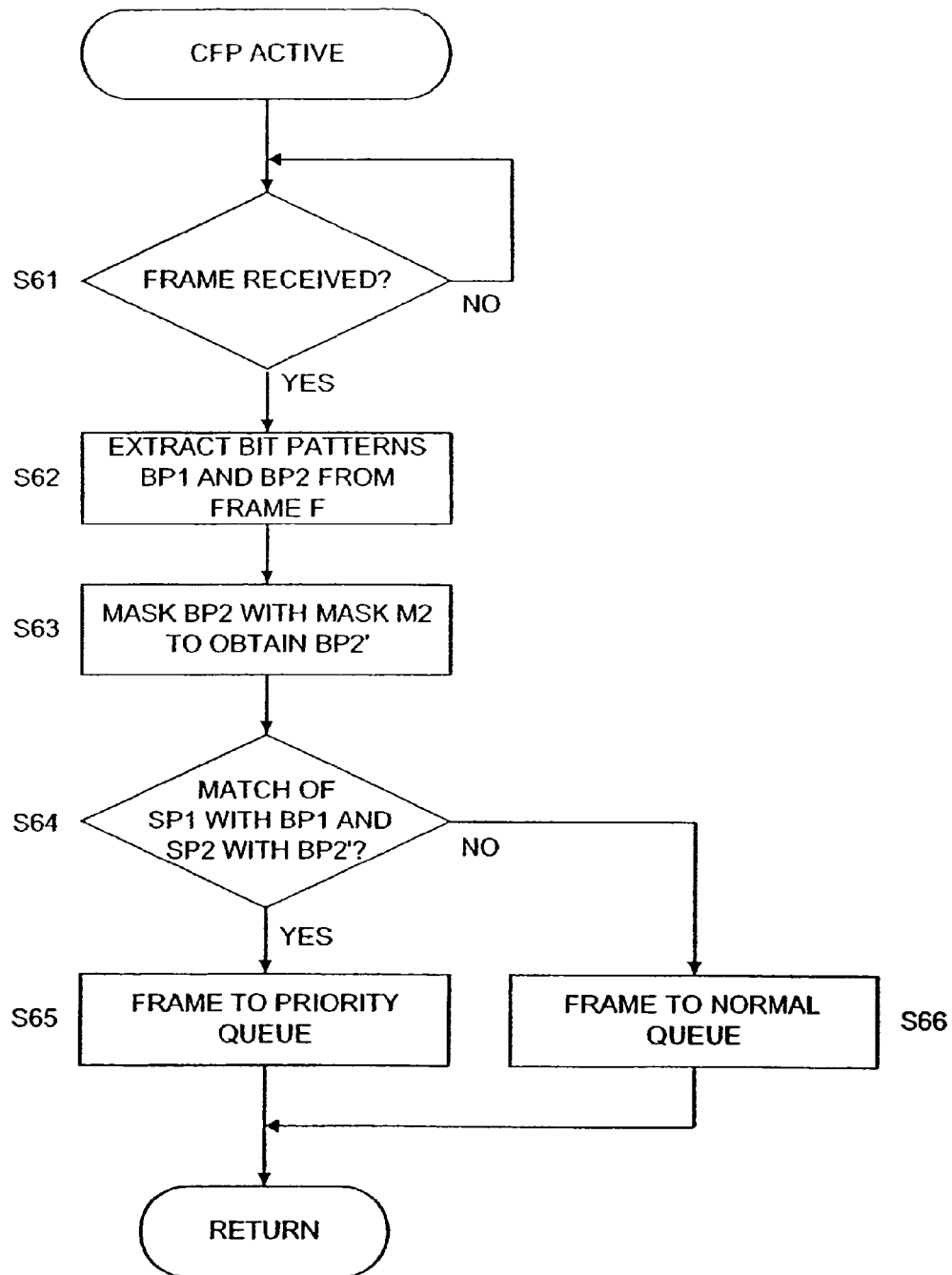


FIG. 6

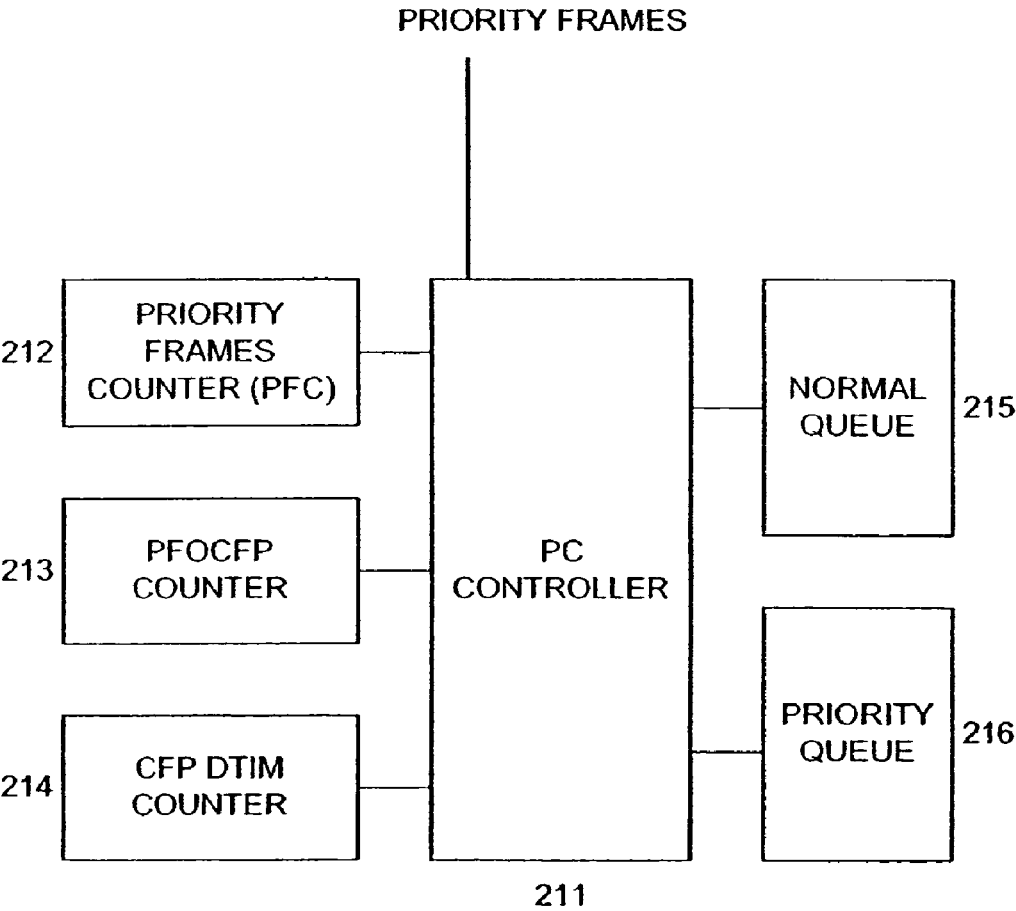


FIG. 7

U.S. Patent

May 20, 2014

Sheet 7 of 10

US RE44,904 E

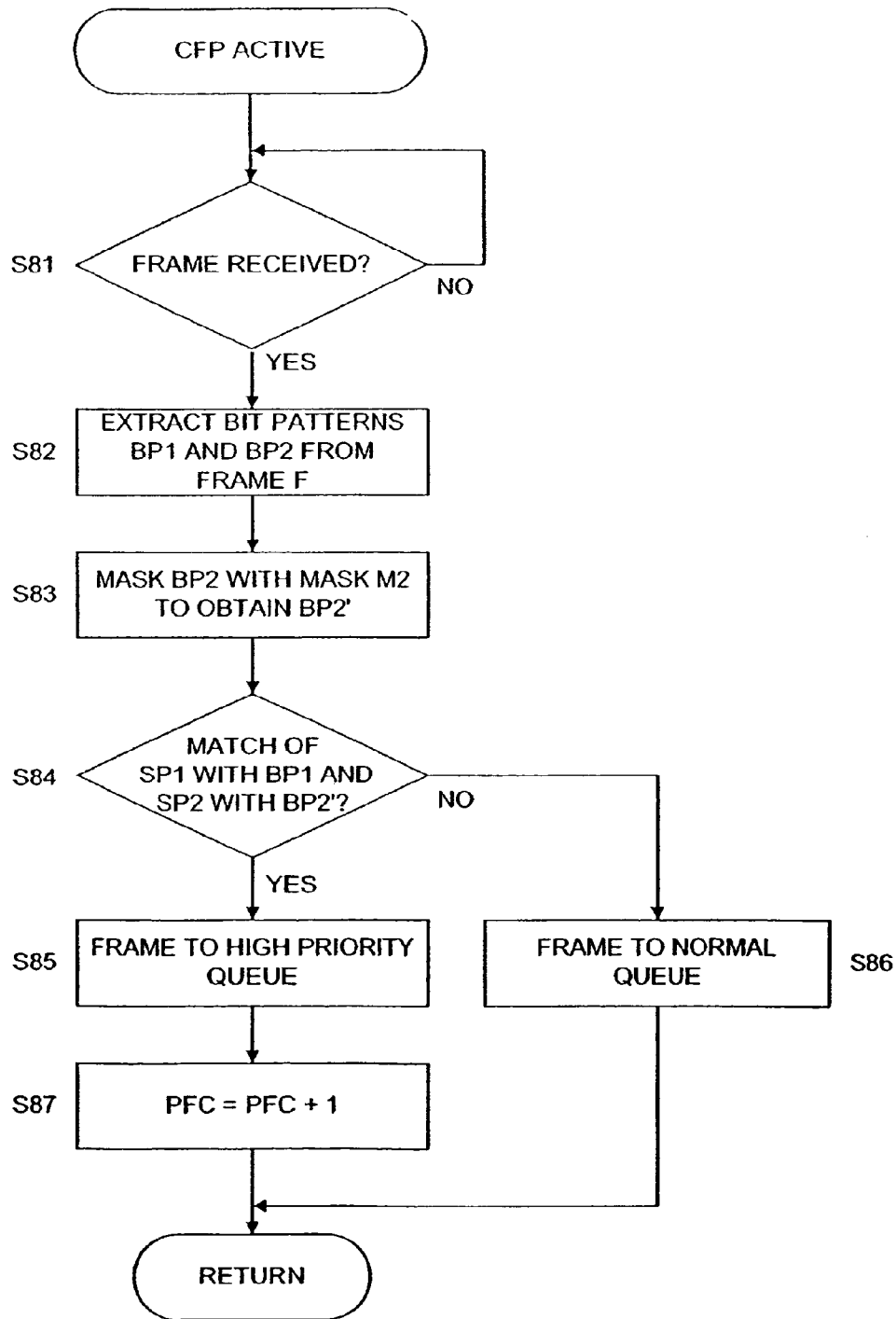


FIG. 8



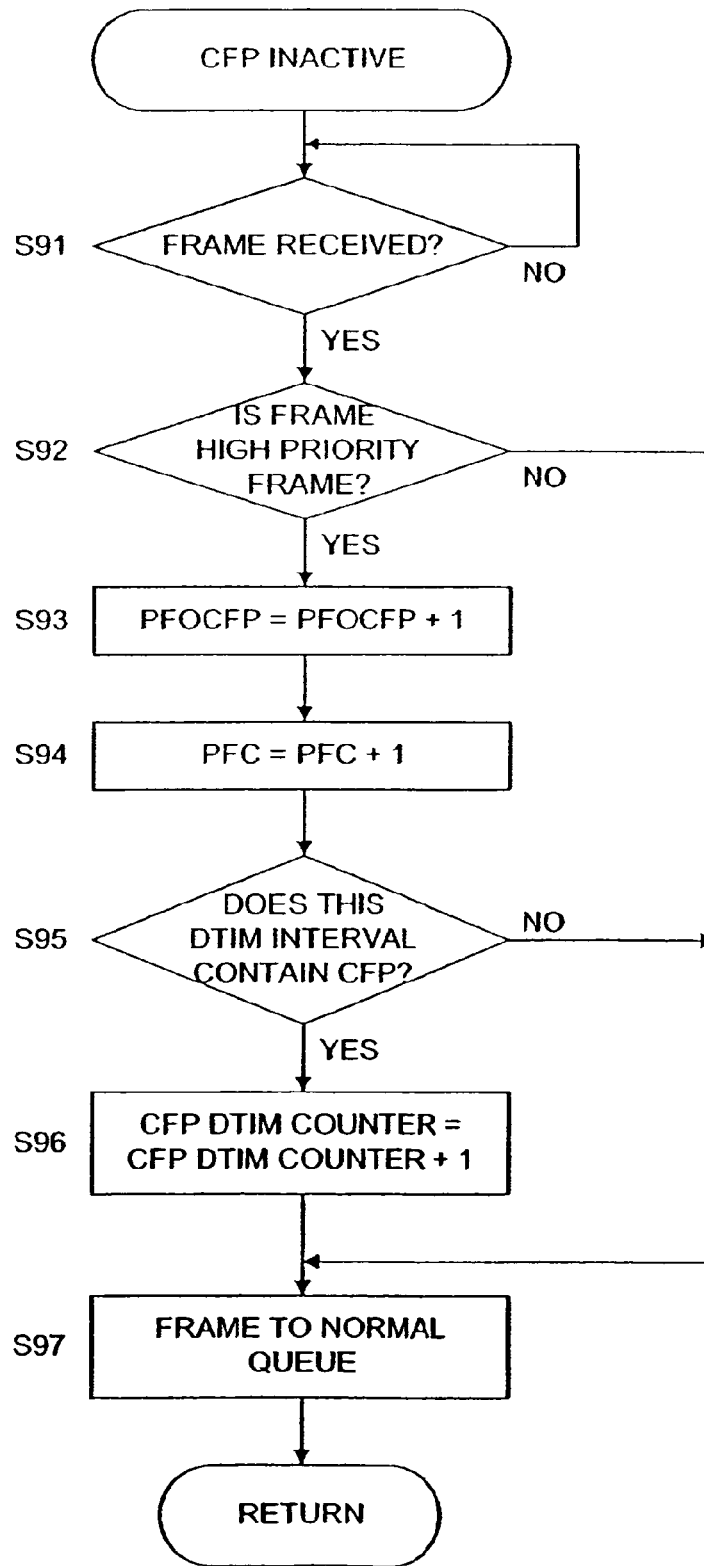
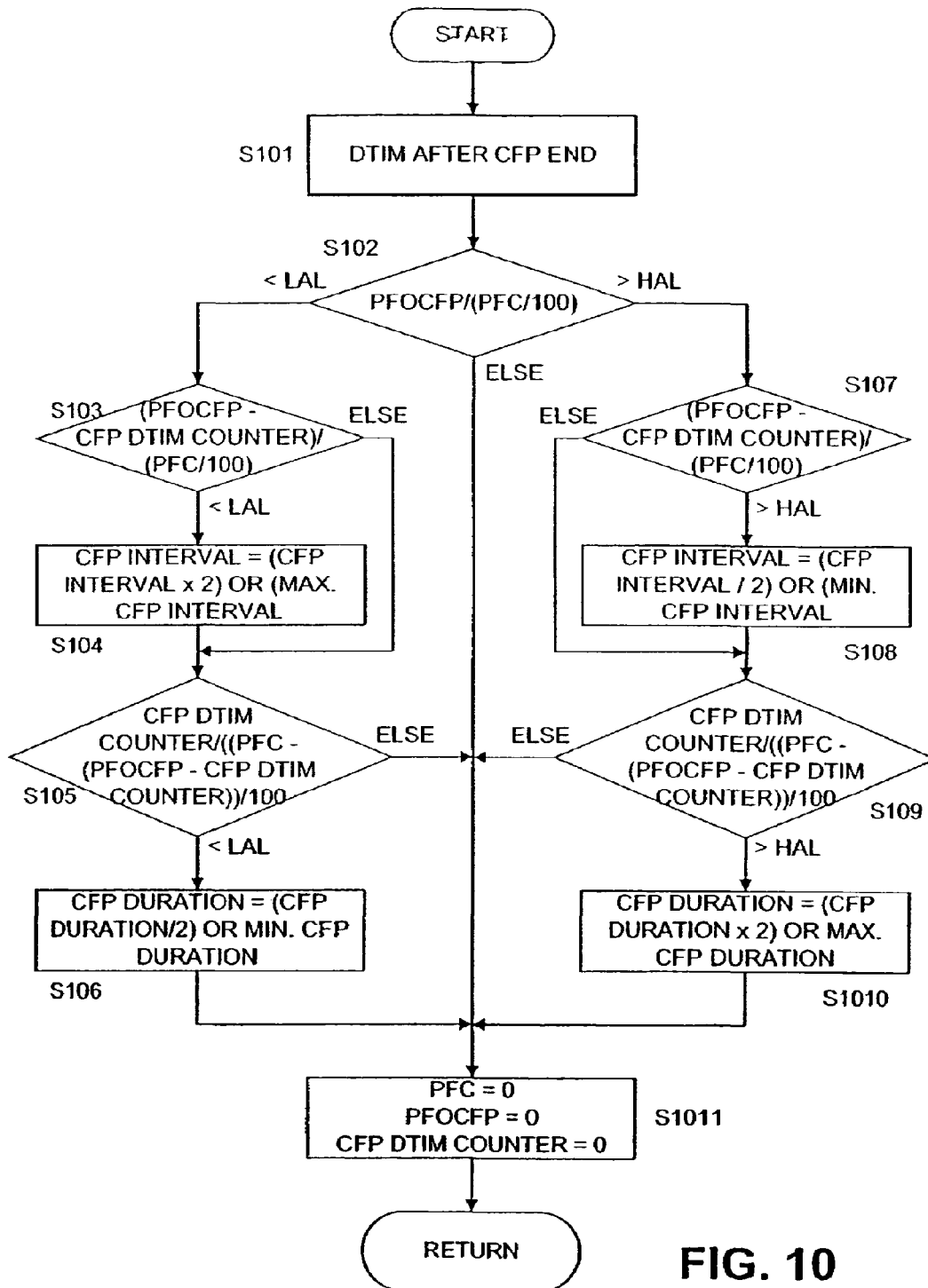


FIG. 9



U.S. Patent

May 20, 2014

Sheet 10 of 10

US RE44,904 E

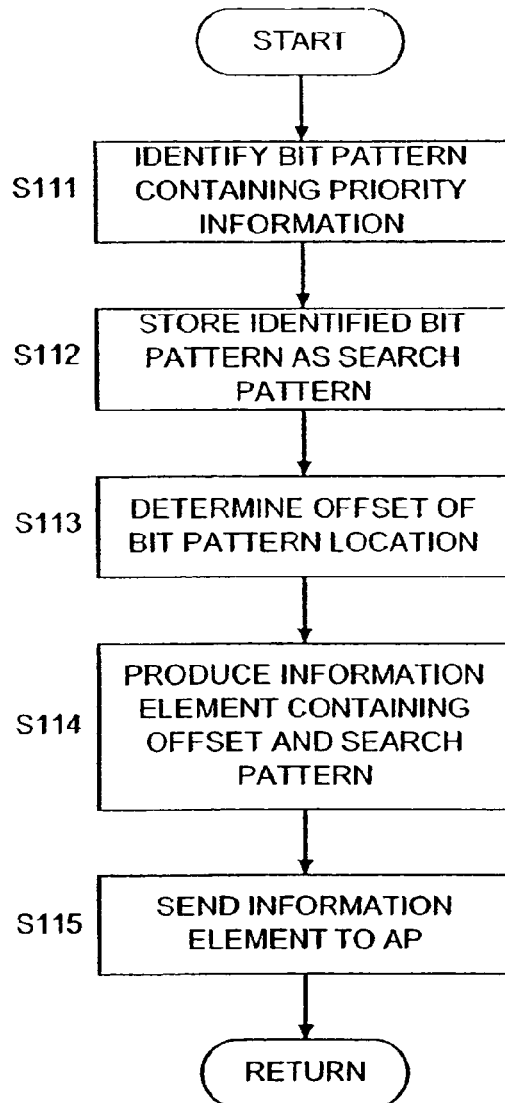


FIG. 11

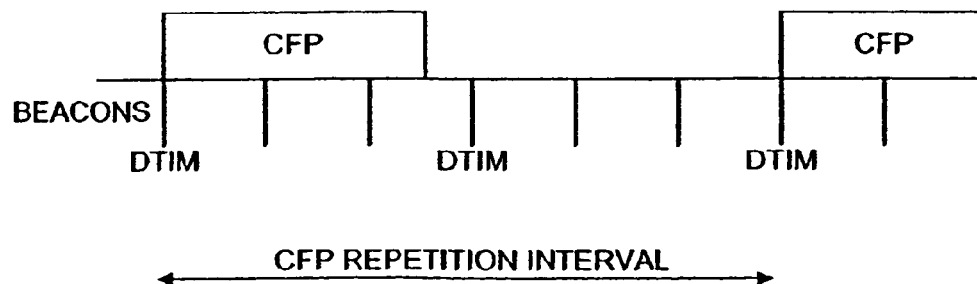


FIG. 12

US RE44,904 E

1

## METHOD FOR CONTENTION FREE TRAFFIC DETECTION

**Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.**

### CROSS-REFERENCE TO RELATED APPLICATIONS

This application *is a reissue of U.S. patent application Ser. No. 11/402,621, filed on Apr. 11, 2006, issued as U.S. Pat. No. 7,555,014, which is a continuation of U.S. patent application Ser. No. 10/167,986, filed Jun. 11, 2002, now U.S. Pat. No. 7,027,465, which is a continuation of International Application PCT/EP99/10097 having an international filing date of Dec. 17, 1999 and from which priority is claimed under all applicable sections of Title 35 of the United States Code including, but not limited to, Sections 120, 363 and 365(c).*

### FIELD OF THE INVENTION

The present invention relates to a method and a device for detecting priority of data frames in a network.

### BACKGROUND OF THE INVENTION

This invention relates in general to the field of telecommunications, more precisely to Wireless Local Area Networks (WLAN) and Electrical and Electronics Engineers (IEEE) 802.11 WLAN standard.

The IEEE 802.11 Wireless Local Area Network specification specifies a so-called Contention Free Period (CFP), which is a period of transmission time that is free from the normal contention based airtime reservation. The length and duration of CFP are configurable parameters in Access Point (AP), so that the start of CFP is repeated after one or more Delivery Traffic Indication Message (DTIM) intervals (see IEEE 802.11 standard). The CFP and its relationship to the so-called Content Period (CP) is schematically illustrated in FIG. 12. As can be seen, a CFP repetition interval contains a Content Free Period (CFP) and a Content Period (CP). Each CFP begins with a beacon frame that contains a DTIM element.

The purpose of this CFP is that it can be used for delivering high priority traffic, which has higher real time requirements than normal traffic. The CFP is controlled by the so-called Point Coordination Function (PCF) in an Access Point (AP). The standard specifies the PCF operation in basic level, but does not specify how the PCF should be controlled or how some traffic should be identified as high priority traffic. These things are considered to be out of the scope of the standard.

Information within data frames is marked as having a high priority by using certain fields in some protocol frames or headers. However, the Access Point (AP) usually processes only frames on the Medium Access Control (MAC) layer such that the AP can not easily access information regarding the priority of certain data blocks within the frames, since this information is processed in higher layers.

Thus, for getting priority information, conventionally the frames which are to be transmitted through an Access Point (AP) had to be searched for these fields which indicate the priority state of the actual data frame. This means that in all frames all fields had to be checked, all the headers had to be

2

analyzed, starting from the outer most headers, until the right field in the header had been found.

Since all frame headers are parsed when detecting priority, this measure has a high reliability.

However, this measure is very complex, takes a long time and requires a large amount of processing. Furthermore, the traffic transferred in WLAN can be practically anything, including complex tunneling protocols. Therefore, all the frame headers and protocols which can be included in the data frames transmitted via the network have to be known. Hence, the amount of information needed for identifying the data is huge. This huge amount of information is typically too heavy to handle in quite small and low price equipment like WLAN access points (AP).

In addition, it has to be considered that every time new protocols are introduced, the access point has to be updated, at least by software updates. This is also required in case protocols already used are changed.

Thus, conventionally such a transmission differentiation based on priority was not conducted at all. That is, the existing systems according to the IEEE 802.11 standard do not separate traffic based on priority. In these conventional systems, the Content Free Period (CFP) is only used to deliver traffic from the Access Point (AP) to stations, treating all frames equally.

### SUMMARY OF THE INVENTION

Therefore, the object underlying the invention resides in removing the above drawbacks of the prior art and to provide a method by which priority traffic can easily be distinguished from normal traffic without the need of a complex processing.

This object is solved by a method for detecting priority of data frames in a network comprising the steps of extracting a bit pattern from a predetermined position in a frame, comparing the extracted bit pattern with a search pattern, and identifying the received frame as a priority frame in case the extracted bit pattern matches with the first search pattern.

Alternatively, the above object is solved by a device for detecting priority of data frames in a network comprising a receiving means for receiving data frames, an extracting means for extracting a bit pattern from a predetermined position of a data frame, a comparing means for comparing the extracted bit pattern with a predetermined search pattern, and an identifying means for identifying the received frame as a priority frame in case the extracted bit pattern matches with the first search pattern.

Thus, a priority which is defined in a higher-level layer can easily be detected by comparing a corresponding bit pattern with a search pattern without further processing of the received frame. By the method and the device according to the invention, simply a bit pattern is extracted at a position in the frame, where the priority information is known to be located. This bit pattern is compared with a search pattern which corresponds to that bit pattern, which would be located at the above position in case that a priority is set for the actual frame. Thus, it is not necessary to process and analyze the received frame, i.e., to process higher-level layers in order to obtain priority information.

Hence, when adopting the IEEE 802.11 WLAN standard, the priority can be detected in the Medium Access Control (MAC) layer which is a low-level layer. That is, the method can easily find higher priority traffic from the stream of MAC layer frames. Therefore, the method does not need any knowledge of the upper layer protocols.

Consequently, according to the method of the invention, certain traffic can be defined to have higher priority than other

## US RE44,904 E

3

traffic when it is handled in an IEEE 802.11 WLAN Access Point (AP). The method is designed so that it is as lightweight as possible to execute in a low cost and possibly low performance AP.

Furthermore, the method is protocol-independent and so flexible that all the configuration may be done in external configuration program and the Access Point does not need to know anything about the processed traffic.

Further advantageous developments are set out below.

In particular, the predetermined position in the frame is defined by the offset of the bit pattern in the frame. Thus, the position of the bit pattern to be extracted and examined can accurately be defined.

Furthermore, the offset and the search pattern are included in an information element. This information element can be produced by an external program such that the device according to the invention and the device performing the method according to the invention does not have to generate the search pattern and the offset. Thus, the structure of the device does not have to be complex.

In addition, in case new protocols or modified protocols are introduced in the network, it is not necessary to reconfigure the network element (i.e., the device) performing the method. It is only necessary to provide new information elements including the new offset and the new search pattern, which can be effected by an external configuration program. For this, it is not necessary to install new software in the network element or to install new hardware. It is not even necessary to shut down the network element for a new configuration. Hence, the method is very flexible.

Moreover, the bit pattern can be masked by using a mask. Then, the masked bit pattern is compared with the search pattern instead of comparing the bit pattern with the search pattern. By this measure, single bits can easily be extracted from the bit pattern. This is advantageous in case the bit pattern is extracted in form of bytes. For example, a bit pattern can include two bytes, whereas for the priority detection only two bits of each byte are required. These two bits can easily be extracted by using the mask.

The mask can also be included in the information element described above.

If necessary, also a plurality of different bit patterns, search patterns, offsets and—optionally—masks can be used to detect priority of the frames. By this measure, priority information can be detected which is located at different positions within a data frame.

Alternatively, a plurality of different priority levels can be provided for the frames. For detecting different priority levels, a plurality of different bit patterns, search patterns, offsets and—optionally—masks can be used to detect the plurality of different priority levels. By this measure, also different priority levels can easily be detected.

Hence, a plurality of different information elements can be used. For example, one certain priority can require a plurality of information elements, while another certain priority can require only one particular information element.

A received frame can be forwarded to a priority queue in case the frame is detected to be a priority frame during a special period for sending priority traffic. The priority queue serves to transmit the data priority frames in the network faster than normal frames. This measure is especially advantageous in an IEEE 802.11 WLAN since in this standard, a Contention Free Period is defined, as described above.

In addition, the duration of the special period for sending priority traffic can be adjusted according statistical information regarding the priority frames sent. Thus, the special

4

period, i.e., the Contention Free Period, can be adjusted corresponding to the load of priority traffic on the network.

Furthermore, for obtaining the statistical information, the total number of priority frames and the number of priority frames outside the special period can be counted. Then, it can be decided on the basis of the count values obtained whether the special period has to be increased or decreased.

In addition, in the IEEE 802.11, a data+CF-poll frame is defined. Preferably, this data+CF-poll frame can be used for transmitting priority frames in case of a symmetrical high priority traffic between the Access Point and stations in the network.

Furthermore, the invention proposes a method for generating priority detecting information necessary for the above method and device. This method comprises the steps of analyzing a data frame, identifying a bit pattern indicating a priority state, defining the identified bit pattern as a search pattern, and locating the bit pattern within the data frame. By this method, the necessary priority detection information can easily be provided. For example, this method can be employed by a configuration program that is externally run, for example, in one of the wireless stations which are connected by air with the Access Point.

The above method for generating priority detecting information may further comprise the steps of determining the offset of the location, and producing an information element including the offset and the search pattern. Optionally, also the mask for masking the bit pattern mentioned above can be determined and included in the information element.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

FIG. 1 shows a main system overview;

FIG. 2 shows a process for checking priority of frames according to a first embodiment;

FIG. 3 shows an example for a frame to be examined by the process according to the first embodiment;

FIG. 4 shows a frame priority detecting device according to the first embodiment;

FIG. 5 shows an example of pattern matching with two different information elements according to a second embodiment;

FIG. 6 illustrates a flow chart of a frame sending procedure during Content Free Period (CFP) according to the second embodiment;

FIG. 7 shows relevant parts of a Point Coordinator (PC) according to a third embodiment;

FIG. 8 illustrates a flow chart of a frame sending procedure during Content Free Period (CFP) according to the third embodiment;

FIG. 9 illustrates a flow chart of a frame sending procedure during contention period according to the third embodiment; and

FIG. 10 illustrates a flow chart of a procedure for CFP parameter tuning according to the third embodiment;

FIG. 11 shows a flow chart of a method for obtaining priority detection information; and

FIG. 12 illustrates the relationship between Content Free Periods (CFP) and Content Periods (CP) according to IEEE 802.11.

## DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following, preferred embodiments of the invention are described in more detail with reference to the accompanying drawings.

## US RE44,904 E

5

FIG. 1 shows an overview of the main system used in the embodiments. The system is a normal IEEE 802.11 Basic Service Set (BSS) containing one Access point (AP) 2 and one or more wireless stations (STA) 3 to 5. The AP may or may not be connected to another wired or wireless network 1. The purpose of the AP 2 is to transmit the traffic between the wireless stations or between wireless stations and the network 1 which is connected to the AP 2.

All the network components function according to the IEEE 802.11 standard. This presented set-up is a typical representation of the coverage area of one AP. The whole wireless network usually consists of several of these kinds of subsystems. An external configuration program may run in one of the stations in the wireless network or it may reside in some other host and be connected to AP with a wire. In this example, the configuration program is executed in the wireless station 3.

In the following, a first embodiment which shows the basic idea of the invention is described with respect to the flow chart shown in FIG. 2 and an example for a Medium Access Control (MAC) layer frame shown in FIG. 3.

The procedure shown in FIG. 2 is executed by the Access Point AP 2 every time a Medium Access Control (MAC) layer frame has been received.

In step S1, the AP 2 extracts a bit pattern from a given position in the received frame. The bit pattern can be a pattern of two bytes, for example. However, the length of the bit pattern can be selected arbitrarily. The extracted bit pattern is indicated by BP in FIG. 2. In step S2, the extracted bit pattern BP is compared with a predetermined search pattern SP. If in step S3 it is decided that both patterns match, it is determined in step S4 that the actual frame is a priority frame. On the other hand, if it is decided in step S3 that both patterns do not match, it is determined in step S5 that the actual frame is not a priority frame. After identifying the priority of the frame, the frame can be treated according to the identified priority.

Thus, the frame can easily be examined whether it is a priority frame or not without the need for analyzing the data format in the MAC layer frame itself, i.e., without knowing protocols of the higher layers.

The position of the bit pattern to be extracted is defined by the offset OS from the start of the MAC frame, as shown in FIG. 3. Thus, the AP 2 requires only information regarding the offset OS and the search pattern SP for checking priority of certain MAC frames.

This information can be provided by an external configuration program. The configuration program can be executed in one of the wireless stations, for example. Alternatively, it can be executed in any suitable network element, including the Access Point itself. For this configuration program it is necessary that the bit positions of the priority information which are usually set in higher layers are known. Thus, by providing the AP with the offset, the AP does not have to process the frame in order to identify priority information. It is only necessary to obtain the corresponding bit pattern.

In the first embodiment, the configuration program is executed in the wireless station STA 3. The configuration program produces information elements which contain the above-described information regarding the offset OS and the search pattern SP necessary to identify the priority state of certain MAC frames. These information elements are transmitted to the AP 2.

FIG. 4 shows the relevant parts of the Access Point 2 in more detail. Reference numeral 22 denotes a frame receiver by which frames are received from the wired or wireless network 1 and also from the wireless stations 2 to 5. Reference numeral 23 denotes a bit pattern extractor by which the

6

bit pattern BP described above is extracted from a predetermined position. The position is defined by the offset OS, as mentioned above, and the offset is stored in an offset memory 27 which is accessed by the bit pattern extractor 23. The extracted bit pattern BP is forwarded to a comparator 24 which compares the extracted bit pattern BP with the search pattern SP. The search pattern SP is stored in a search pattern memory 25 which is accessed by the comparator 24. The comparison result is supplied to a priority identifying means 26 which identifies the actual frame F as a priority frame in case the comparison results indicates that the bit pattern BP matches the search pattern SP. Thus, the Access Point (AP) 2 can detect priority frames and can treat them correspondingly.

As mentioned above, the external configuration program provides information elements which each comprise an offset OS and a search pattern SP. These information elements are received by an information element receiver 28. The receiver 28 analyzes the information element and supplies the detected offset OS to the offset memory 27 and the detected search pattern SP to the search pattern memory 25.

The first embodiment described above illustrates the basic operation according to the invention. The second embodiment described in the following describes a further, more detailed example for the high priority traffic detection method in which the Content Free Period (CFP) defined in IEEE 802.11 standard is used for transmitting detected high priority frames.

According to IEEE 802.11, the Content Free Period (CFP) is a period which is reserved for transmitting high priority traffic, as described above in the introductory part with respect to FIG. 12. The CFP is controlled by a Point Coordinator (PC) 21 which is arranged in the Access Point (AP) 2 shown in FIG. 1. If the high priority traffic is transferred only from the AP 1 to the wireless stations (i.e., in a typical client-server application case), the CFP may be used only for delivering data from the AP to wireless stations. But, if the nature of the high priority traffic is interactive (like a videoconference, for example), the PC 21 must also poll wireless stations to permit them to transmit also during the CFP. See IEEE 802.11 standard for more detailed description about this basic functionality of IEEE 802.11 standard.

The AP 2 receives MAC layer frames either from the wireless station or from the connected wired network. If the destination of the frame is in the wireless network, the AP will check whether the frame is high or normal priority traffic. The priority detection requires that the AP 2 is configured with the external configuration program to detect the priority and the required configuration information elements are configured to the AP by the external configuration program. The AP also needs to reformat the MAC level header of the frame or encapsulate the frame inside a separate IEEE 802.11 MAC header which is defined in IEEE 802.11. The point when the priority detection check is performed (before or after IEEE 802.11 MAC header formatting) can be left implementation specific.

If the BSS is in a so-called Contention Free (CF) state (i.e., currently there is a Contention Free Period (CFP)) and the frame is a priority frame, the frame is put in a priority transmit queue, otherwise the frame is treated like the normal traffic. During the CFP, all the frames in the priority queue are transmitted before any frames from the normal queue. When the CFP ends, remaining frames in the priority queue are moved to the normal queue and priority queue is flushed.

According to this embodiment, the priority of a MAC layer frame is detected by using one or more information elements which are transmitted to the Access Point (AP) 1. That is, one or more bit patterns with corresponding different offsets are



## US RE44,904 E

7

checked whether they match with one or more different search patterns. Furthermore, the bit patterns extracted from the MAC layer frame are also masked by using a mask. The mask is also contained in an information element. Thus, the information element according to the second embodiment comprises the offset and the search pattern as according to the first embodiment, and in addition a mask. The mask serves to obtain only particular bits in the extracted bit pattern and is optional.

The operation according to the second embodiment is described by referring to FIGS. 5 and 6. It is noted that for simplifying the illustration, the second embodiment is described with reference to the case that the priority is detected by using two information elements.

In FIG. 5 it is shown that two bit patterns BP1 and BP2 are extracted from the MAC layer frame F. The first bit pattern BP1 is extracted with an offset OS1. As illustrated, the first bit pattern matches with the first search pattern SP1. For the first bit pattern BP1, no mask has been specified (i.e., no masking is performed).

However, for the second bit pattern BP1 a mask M2 is specified. In this example, the mask is M2=00010000 such that only the fourth bit is passed through. The resultant bit pattern BP2' is then compared with the second search pattern SP2. Here, the second search pattern SP2 and the masked bit pattern BP2' match. Since also the first search pattern SP1 matches with the first bit pattern BP1, it is decided that the actual frame F is a high priority frame.

According to the second embodiment, the frame F which has been detected as a priority frame, is transmitted in the Contention Free Period (CFP). That is, it is put on a high priority queue. This process is described in the following by referring to the flow chart shown in FIG. 6.

The process shown in this flow chart is performed during the Content Free Period, i.e., in case the CFP is active. In step S61, the Access Point (AP) 2 waits for receiving a frame which is to be transmitted further to the wireless stations 3 to 5 (FIG. 1). In step S62, the bit patterns BP1 and BP2 are extracted from the frame F, as shown in FIG. 5. In step S63, the bit pattern BP2 is masked with the mask M2 to obtain a bit pattern BP2', as described above. Since no mask has been specified for the first bit pattern BP1, no corresponding step for the first bit pattern BP1 is performed.

Then, in step S64, it is checked whether both bit patterns BP1 and BP2' match with the search patterns SP1 and SP2, respectively. If SP1 and BP1, and SP2 and BP2' respectively match, it is decided that the received frame F is a high priority frame, and the frame F is put in the priority queue (step S65). This is effected by the Point Coordinator (PC) 21 arranged in the Access Point (AP) 2. If the patterns do not match (NO in step S64), the received frame F is put in the normal queue, as shown in step S66.

As described above, the Point Coordinator (PC) 21 puts a priority frame in the priority queue in case the Contention Free Period (CFP) is active. However, in case the CFP is inactive, the frame goes to the normal queue so that it does not have to wait for the CFP to start. When the CFP starts, the PC flushes the normal queue and places the unsent high priority frames in the priority queue. Thus, when the Point Coordinator (PC) 21 notices that the frame which should be sent is a high priority frame, it puts this frame in the normal or high priority queue depending on the current state of the network.

As mentioned above, the use of two information elements is only an example. The number of information elements can be more than two. By using a plurality of information elements, it is also possible to distinguish between different priority levels. For example, the configuration program can

8

give the following data to the Access Point by which three priorities (i.e. priority 1, priority 2 and priority 3) can be distinguished. It is noted that these three priorities can each represent different priority levels (e.g., priority 1 represents the highest priority while priority 3 has the lowest) or can represent equal priority levels.

Priority 1 information:

Information element 1: offset 1 and search pattern 1

Information element 2: offset 2 and search pattern 2

Information element 3: offset 3 and search pattern 3 . . .

Information element n: offset n and search pattern n

Priority 2 information:

Information element 1: offset 1 and search pattern 1

Priority 3 information:

Information element 1: offset 1 and search pattern 1

Information element 2: offset 2 and search pattern 2

The AP then checks whether a received frame matches with all the information elements of the first group containing the information elements for priority 1. That is, for each information element it is checked whether a bit pattern at the offset included in the information element matches with the search pattern included in the information element. If this is the case for all information elements, then the frame has the priority 1.

If the frame does not match with all information elements listed in the first group, then the AP tests the same frame with all the information elements (one, in this example) of the second group containing the information elements for priority 2. If the bit pattern extracted at the offset 3 in the frame matches with the search pattern 3 included in information element 3, it is decided that the frame has the priority 2.

However, if the patterns do not match, then the AP checks the priority 3 information. That is, the frame is checked whether it matches with information elements 1 and 2. If this is the case, the frame has the priority 3. If the frame still does not match, it has no priority.

Next, a third embodiment is described, according to which the Point Coordinator (PC) 21 collects statistics about the high priority traffic sent and adjusts the parameters for the CFP.

In detail, the PC 21 counts the high priority packets during the every so-called Delivery Traffic Indication Message (DTIM) interval (see IEEE 802.11 WLAN standard). Furthermore, it also counts how much of those packets are transmitted outside the CFP and how much during the DTIM interval containing CFP but outside CFP. The PC saves statistics of the previous N DTIM intervals, where N is at least the CFP repeating interval. The PC then checks the statistics after every DTIM interval that contains CFP and adjusts the CFP length and interval accordingly. The frame handling and statistics collection during the CFP is presented in FIG. 8 and during the contention period in FIG. 9.

The PC 21 according to the third embodiment is shown in FIG. 7 in greater detail. As derivable therefrom, the PC comprises a plurality of counters which are used by a PC controller 211 to control the CFP. A priority frames counter (PFC) 212 serves to count all priority frames received. A counter for priority frames outside CFP (PFOCFP) counter 213 serves to count all priority frames which are received during the contention period, i.e., when CFP is inactive. A CFP DTIM counter 214 serves to count all priority frames which are received in an DTIM interval containing a Contention Free Period (CFP). As mentioned above, the PC 21 forwards the received priority frames either to the normal queue 215 or to the priority queue 216 depending on the current state of the network.

The flowchart shown in FIG. 8 is almost the same as in FIG. 6. The steps S81 to S86 correspond to the steps S61 to S66 of FIG. 5. Thus, an unnecessary repetition is omitted here. How-



## US RE44,904 E

9

ever, in addition to the flow chart shown in FIG. 6, a new step S87 is performed in case patterns SP1 and BP1, and SP2 and BP2' match. In this step S8, the priority frame counter (PFC) 212 is incremented each time it is decided that an actual frame is a high priority frame.

FIG. 9 shows a flowchart representing a process performed during the content period, i.e., when the CFP is inactive. Here, all received frames are put in the normal queue. In case of a high priority frame, several values are counted by the counters of the Point Coordinator (PC) 21 for providing statistical information.

In detail, in step S91 it is waited for a frame, similar to step S81 of FIG. 8. In step S92, the priority is detected in the way as described in the first or second embodiment. If the actual frame is a normal frame with no priority, the flow advances to step S97 in which the frame is put to the normal queue 215. If, however, the actual frame is a priority frame, the flow advances to step S93 in which PFOCFP counter 213 is incremented. Furthermore, in step S94 also the priority frames counter 212 is incremented.

In step S95 it is checked whether the actual DTIM interval contains a Content Free Period (CFP). If this DTIM interval contains a CFP, the CFPDTIM counter 214 is incremented in step S96 before the flow advances to step S97. Otherwise, the flow advances directly to step S97. Thereafter, the routine is ended.

The statistical information regarding the priority frames are used as described in the following with reference to FIG. 10.

As shown in FIG. 10, the procedure is started in an DTIM interval after the end of the Content Free Period (step S101). In step S102, the percentage of priority frames sent outside of the CFP is checked. Depending on the result, different processes are executed, as described next.

If the percentage of high priority traffic sent outside of CFP is higher than a certain high alarm level HAL, the PC 21 will start corrective actions. These processes are illustrated on the right side of the flow chart shown in FIG. 10.

The alarm level is 100%—percentage of the high priority traffic that must be sent inside the CFP in any case. For example, if it is known that the traffic which requires an almost real-time treatment requires a priority traffic of 30%, the alarm level is set to 70%. The alarm level can be fixed or it can be dynamically adjustable.

When the alarm level HAL is reached, the PC will next check the percentage of high priority traffic sent during the DTIM intervals not containing the CFP. This is effected in step S107 in which the difference between the count values of the PFOCFP counter 213 and the CFP DTIM counter 214 is calculated, wherein the difference is brought in relation to the value of the priority frames counter (PFC) 212. If it is more than the alarm level HAL, the PC will make the CFP interval to be half of the original (if it is not already one DTIM interval), as described in step S108.

Next, in step S109, the PC 21 will check if the percentage of high priority traffic sent outside of the CFP during the DTIM intervals containing CFP is also higher than the alarm level. This percentage P is calculated as follows:

$$\text{CFP DTIM counter} / (\text{PFC} - (\text{PFOCFP} - \text{CFP DTIM counter})) / 100$$

If this percentage is higher than the alarm level, the PC 21 will double the duration of the CFP (if not already maximum possible) in step S1010. The alarm level used in the different steps may be the same or different according to the wanted system behavior.

10

If it is decided in step S102 that the percentage of high priority traffic sent outside the CFP drops below a low alarm level LAL, the PC 21 will start decreasing the CFP in order to give the normal traffic also a reasonable chance to be delivered in time. The low alarm level LAL is the percentage of the high priority traffic that can be sent outside the CFP if needed. In order that the system can work smoothly, the low alarm level should be less than 100%—high alarm level HAL.

When the alarm level LAL is reached, the PC 21 will next check what is the percentage of high priority traffic sent during the DTIM intervals not containing the CFP in step S103 which corresponds to step S107 described above. If it is less than alarm level, the PC will make the CFP interval to be double of the original in step S104. Next, the PC 21 will check if the percentage of high priority traffic sent outside of the CFP during the DTIM containing CFP is also lower than the alarm level LAL. This is effected in step S105 which corresponds to step S109 described above. If this percentage is lower as the alarm level LAL, the PC 21 decreases the duration of the CFP with the amount of the previous addition in step S106. The alarm level LAL used in the different steps may be the same or different according to the wanted system behavior.

If it is decided in step S102 that the percentage of priority frames outside the Content Free Period (i.e., the count value of the PFOCFP counter 213 with respect to the count value of the priority frame counter 212) is between the low alarm level LAL and the high alarm level HAL, the flow advances directly to step S1011 in which all counters 212, 213 and 214 are reset. Then, the procedure is ended.

Next, a fourth embodiment is described. The structure and procedures according to this embodiment is similar to the embodiments described above. However, in this embodiment the nature of the high priority traffic is checked. In particular, it is considered whether the high priority traffic is symmetrical, i.e., whether the high priority traffic from a wireless station to the Access Point (AP) 2 is the same or almost the same as the high priority traffic from the AP 2 to the wireless station.

During the Content Free Period (CFP) the wireless stations (terminals) are not allowed to transmit unless the PC 21 polls them. Therefore, they will register themselves to PC to be placed in a polling list. In order to get the best benefit from this traffic control, wireless stations in the WLAN must be able to identify the high priority traffic and send that traffic during the CFP.

In case of the symmetrical high priority traffic between the AP 2 and the wireless stations, the configuration information (from the external configuration program) contains a field telling that this is symmetrical high priority traffic. When the Point Coordinator (PC) 21 in the AP 2 detects that the high priority traffic is symmetrical and the receiving station is pollable during the Content Free Period (i.e., is CF-pollable), it will send it to the terminal inside a so-called data+CF-poll frame instead of normal data frame during the CFP. The data+CF-poll frame is a special data frame, defined in the IEEE 802.11 standard, that allows the receiving station send one data frame during the CFP after receiving the data +CF-poll frame. During the contention period, the symmetrical traffic does not cause any special processes. The use of data+CF-poll frame enables equal high priority data delivering performance to both directions.

The PC 21 must ensure that other wireless stations in the polling list gets polled according to the standard even when delivering symmetrical high priority traffic.

## US RE44,904 E

## 11

In the following, the configuration program used for generating priority detection information used in the above embodiments is described in more detail.

The method adopted in the configuration program is described by referring to the flowchart shown in FIG. 11.

In step S111, a bit pattern (consisting, for example, of one or two bytes) which indicates the priority information is identified in the data frame. The identified bit pattern is defined as the search pattern (SP) in step S112. In step S113, the location, that is, the offset of the identified bit pattern (i.e., the search pattern) inside the data frame is determined. Thereafter, an information element containing the determined offset and the identified search pattern is produced in step S114. Finally, in step S115 the information element is sent to the Access Point and the routine ends.

In a similar way, also the optional mask (as used in the second embodiment) can be obtained. Therefore, an additional step is required which is performed after the bit pattern identifying step S112 such that the mask is defined. It is also possible to produce a plurality of information elements, as used in the second and third embodiment, also by taking into account a plurality of different priority levels.

Next, an example is described in which frames (containing IP packets) to be sent to a particular IP-address should have high priority. In this case, the identification of the search patterns and the location of the search patterns can be performed as follows: The configuration program knows that the offset to the destination IP-address from the beginning of the IP packet (as an example for a data frame) is 32 bytes and the offset from the beginning of the ethernet (version 2) frame to beginning of the IP packet is 14 bytes. Thus, the actual offset of the IP-address is 46 bytes. The search pattern is the IP-address in question. Thus, the necessary information for an information element can easily be extracted.

In other cases, it might be necessary that the configuration program analyzes frames in order to obtain the relevant information.

The location for performing the above method within the network can be arbitrarily chosen. It may be located in some station in the wireless network, it may be centralized in a place in the wired network, or it may be connected to the AP with a separate cable. In some cases, the configuration program may also be run in the AP, but in this way the benefit of the configuration program being external will be lost.

Preferably, the location where the above method, i.e., the external configuration program can be performed is in one of the wireless stations 2 to 5. In this way, the program can also "snoop" the traffic and check whether the traffic is correctly recognized by the AP, that is, whether the high priority traffic is correctly treated. This is because in the wireless stations, the data sent with the frames are processed and, thus, it is clear whether a received frame is a priority frame or not.

When placed in the WLAN, the configuration program can also make corrections to the AP configurations (i.e., the information elements sent to the AP) based on a traffic monitoring in the WLAN. The configuration program can be run in some notebook PC in WLAN, for example.

In rather large networks, however, the best place for the configuration program is in the wired network, where all the access points of the network can be controlled with a single configuration program.

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiments of the invention may vary within the scope of the attached claims. For example, the embodiments can be arbitrarily combined.

## 12

In particular it has to be noted that the above description of the embodiment has been made basically with respect to the IEEE 802.11 WLAN standard. However, it has to be noted that this is only an example and that it is to be understood that the invention can also be applied to other suitable network situations.

Furthermore, in the above embodiments it was basically distinguished between priority frames and normal frames, i.e., between frames with priority and frames without priority. However, it is also possible to distinguish between a plurality of different priority levels. For example, the second embodiment can be modified such that the two bit patterns are used to distinguish between three different priority levels (no priority—medium priority—high priority). Also, different masks for one bit pattern can be used to distinguish between different priority levels.

The invention claimed is:

1. A method comprising

extracting a bit pattern from a predetermined position in a frame[.];

comparing said extracted bit pattern with a search pattern[.];

identifying a received frame as a priority frame in case said extracted bit pattern matches with said search pattern[.]; forwarding said received frame to a high priority queue in case said frame is detected to be a high priority frame during a special period for sending priority traffic[.]; and adjusting the duration of the special period for sending priority traffic according to statistic information regarding sent priority frames.

2. The method according to claim 1, further comprising counting the total number of priority frames; counting the number of priority frames outside said special period; and deciding whether said special period has to be increased or decreased on the basis of the count values obtained in said counting steps.

3. A device comprising

a receiver configured to receive data frames;

an [extracter] *extracter* configured to extract a bit pattern from a predetermined position of a data frame;

a comparator configured to compare said extracted bit pattern with a predetermined search pattern; and

an identifier configured to identify said received frame as a priority frame in case said extracted bit pattern matches with said first search pattern,

wherein a controller is configured to forward said received frame to a high priority queue in case said frame is detected to be a high priority frame during a special period for sending priority traffic, and

said controller is configured to adjust the duration of the special period for sending priority traffic according to statistical information regarding sent priority frames.

4. The device according to claim 3, wherein said controller, in order to obtain said statistic information, is configured to access a priority frames counter for counting the total number of priority frames and a counter for counting priority frames outside said special period, said controller configured to decide whether said special period has to be increased or decreased on the basis of the count values obtained in said counting.

5. A device comprising

means for extracting a bit pattern from a predetermined position in a frame[.];

means for comparing said extracted bit pattern with a search pattern[.];

## US RE44,904 E

13

means for identifying a received frame as a priority frame in case said extracted bit pattern matches with said search pattern[. and];

means for forwarding said received frame to a high priority queue in case said frame is detected to be a high priority frame during a special period for sending priority traffic[.]; and

means for adjusting the duration of the special period for sending priority traffic according statistic information regarding sent priority frames.

6. A memory having a program stored thereon for execution in a device by carrying out the method of claim 1.

7. A method comprising:

detecting a received frame is a priority frame based, at least in part, on information in the received frame, including extracting a bit pattern from a predetermined position in the received frame and comparing the extracted bit pattern with a search pattern, and wherein the detecting is based on a match between the extracted bit pattern and the search pattern;

transmitting the received frame in a transmit period reserved for priority frames in response to the detecting; and

adjusting a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames.

8. The method of claim 7, further comprising forwarding the received frame to a priority queue for transmission in the transmit period reserved for priority frames.

9. The method of claim 8, further comprising forwarding the received frame from the priority queue to a normal queue for transmission outside of the transmit period reserved for priority frames in response to an expiration of the transmit period reserved for priority frames.

10. A method comprising:

detecting a received frame is a priority frame based, at least in part, on information in the received frame;

transmitting the received frame in a transmit period reserved for priority frames in response to the detecting;

adjusting a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames; and

forwarding the received frame to a normal queue for transmission outside of the transmit period reserved for priority frames when the transmit period reserved for priority frames is unavailable.

11. A method comprising:

detecting a received frame is a priority frame based, at least in part, on information in the received frame;

transmitting the received frame in a transmit period reserved for priority frames in response to the detecting;

adjusting a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames; and

counting a total number of priority frames; and

counting a number of the priority frames transmitted outside of the transmit period reserved for priority frames, wherein the adjusting of the transmit period is based on a ratio of number of the priority frames transmitted outside of the transmit period reserved for priority frames and the total number of priority frames.

12. A method comprising:

detecting a received frame is a priority frame based, at least in part, on information in the received frame;

transmitting the received frame in a transmit period reserved for priority frames in response to the detecting;

14

adjusting a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames,

wherein the statistic information regarding sent priority frames is based on a percentage of priority frames transmitted outside of the transmit period reserved for priority frames to a total number of priority frames transmitted.

13. A device comprising:

a controller to detect a received frame is a priority frame based, at least in part, on information in the received frame; and

a priority queue configured to transmit the received frame in a transmit period reserved for priority frames, wherein the controller is configured to adjust a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames, wherein the controller is configured to extract a bit pattern from a predetermined position in the received frame, to compare the extracted bit pattern with a search pattern, and to detect a received frame is a priority frame based, at least in part, on a match between the extracted bit pattern and the search pattern.

14. The device of claim 13, wherein the controller is configured to forward the received frame to the priority queue for transmission in the transmit period reserved for priority frames.

15. The device of claim 13, further comprising a normal queue configured to transmit the received frame outside of the transmit period reserved for priority frames.

16. The device of claim 15, wherein the controller is configured to transfer the received frame from the priority queue to the normal queue in response to an expiration of the transmit period reserved for priority frames.

17. A device comprising:

a controller to detect a received frame is a priority frame based, at least in part, on information in the received frame; and

a priority queue configured to transmit the received frame in a transmit period reserved for priority frames, wherein the controller is configured to adjust a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames, wherein the controller is configured to count a total number of priority frames, to count a number of the priority frames transmitted outside of the transmit period reserved for priority frames, and to adjust the transmit period reserved for priority frames based on a ratio of number of the priority frames transmitted outside of the transmit period reserved for priority frames and the total number of priority frames.

18. A device comprising:

a controller to detect a received frame is a priority frame based, at least in part, on information in the received frame; and

a priority queue configured to transmit the received frame in a transmit period reserved for priority frames, wherein the controller is configured to adjust a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames, wherein the statistic information regarding sent priority frames is based on a percentage of priority frames transmitted outside of the transmit period reserved for priority frames to a total number of priority frames transmitted.

\* \* \* \* \*

# Exhibit L

---



US007760664B2

(12) **United States Patent**  
**Gupta**

(10) **Patent No.:** **US 7,760,664 B2**  
(45) **Date of Patent:** **\*Jul. 20, 2010**

(54) **DETERMINING AND PROVISIONING PATHS  
IN A NETWORK**

(76) Inventor: **Sanyogita Gupta**, 8 Colasurdo Ct.,  
Edison, NJ (US) 08820-4420

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 1005 days.

This patent is subject to a terminal dis-  
claimer.

5,377,262 A	12/1994	Bales et al.	379/221.06
5,526,414 A	6/1996	Bedard et al.	379/221.01
5,764,740 A *	6/1998	Holender	379/112.05
6,091,720 A	7/2000	Bedard et al.	
6,981,065 B1 *	12/2005	Lu	709/251
7,173,912 B2 *	2/2007	Jaber et al.	370/254
2002/0029298 A1 *	3/2002	Wilson	709/316
2003/0071840 A1	4/2003	Huang et al.	
2003/0189919 A1	10/2003	Gupta et al.	
2004/0107277 A1	6/2004	Levesque et al.	
2005/0097108 A1 *	5/2005	Wang et al.	707/100
2005/0169179 A1 *	8/2005	Antal et al.	370/231
2006/0015617 A1 *	1/2006	Castro et al.	709/226

(21) Appl. No.: **11/101,136**

(22) Filed: **Apr. 7, 2005**

(65) **Prior Publication Data**

US 2006/0067236 A1 Mar. 30, 2006

**Related U.S. Application Data**

(60) Provisional application No. 60/614,609, filed on Sep.  
30, 2004.

(51) **Int. Cl.**  
**H04L 12/28** (2006.01)  
**G06F 15/177** (2006.01)  
**G06F 15/16** (2006.01)

(52) **U.S. Cl.** ..... **370/254**; 370/389; 370/400;  
709/220; 709/249

(58) **Field of Classification Search** ..... 370/235–240,  
370/254–258, 400–401; 709/220, 249  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

4,284,852 A	8/1981	Szybicki et al.	379/221.01
4,669,113 A	5/1987	Ash et al.	379/221.01
4,788,421 A	11/1988	Ogawa et al.	250/201.5
5,297,137 A	3/1994	Ofek et al.	370/403

**OTHER PUBLICATIONS**

International Search Report for PCT/US2005/034418 mailed Dec.  
27, 2006.

European Search Report for European Application 05857725.5,  
dated Aug. 25, 2009.

Notice of Rejection for Japanese Patent Application No. 2007-  
534687, mailed Jul. 31, 2009 (with English Translation).

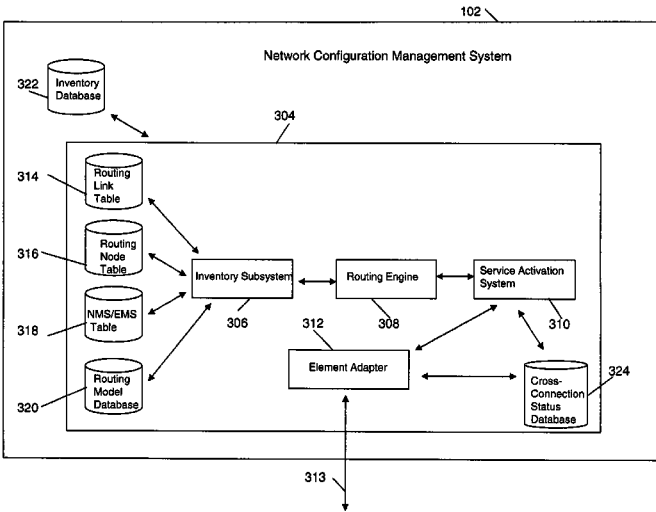
\* cited by examiner

*Primary Examiner*—Tri H Phan

(57) **ABSTRACT**

A network provisioning system for establishing a path between two networks is disclosed wherein a common network device between those networks is modeled as a link between a first network element in one network and a second network element in a second network. A network routing graph is created by an inventory subsystem in a routing manager by inventorying the physical network elements and links in the network. The inventory subsystem then models those elements/links as a plurality of nodes and links between the nodes. At least one common network device, such as a digital cross connect connecting the two networks, is modeled as a link instead of a node. A routing engine then uses the network routing graph, including the link modeled from the common network device, to provision a path between the networks.

**14 Claims, 5 Drawing Sheets**



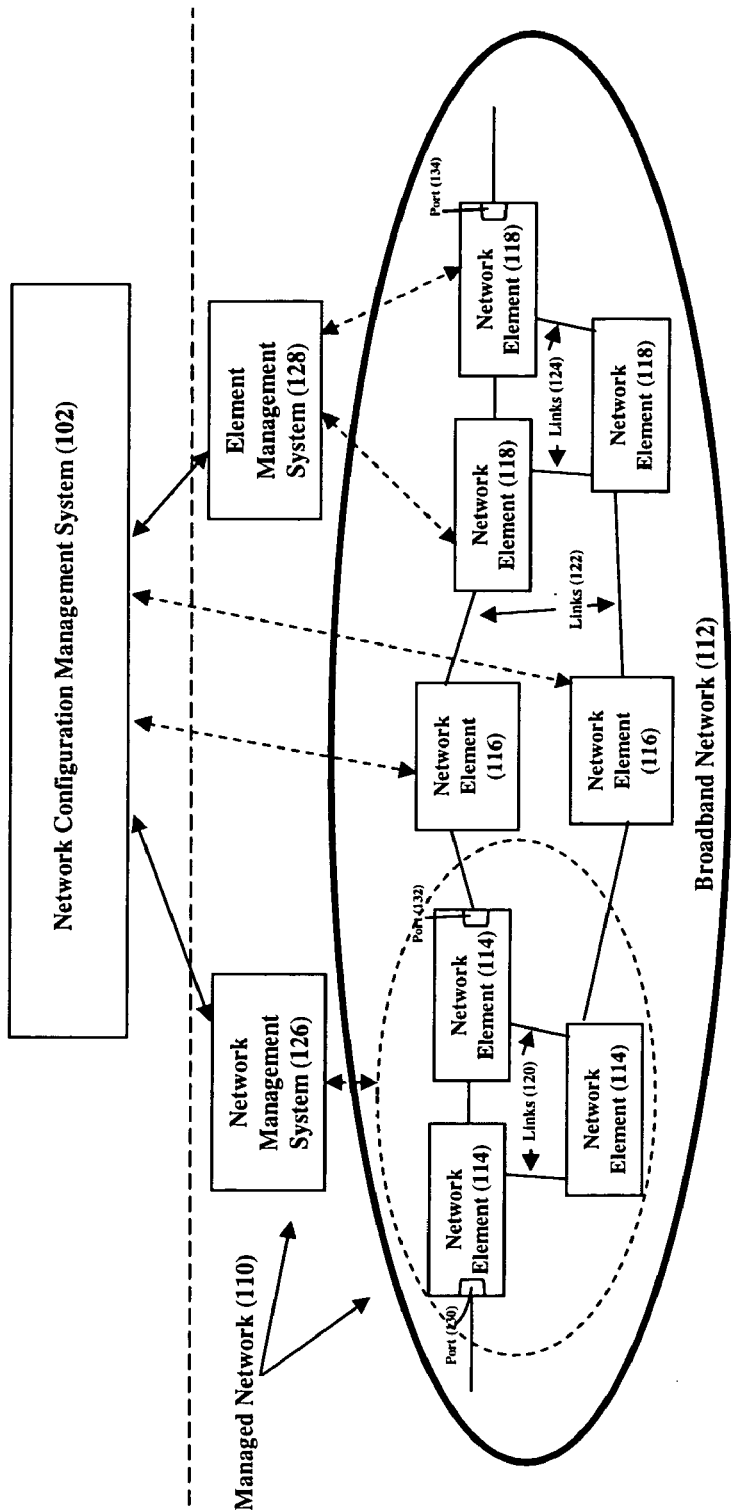
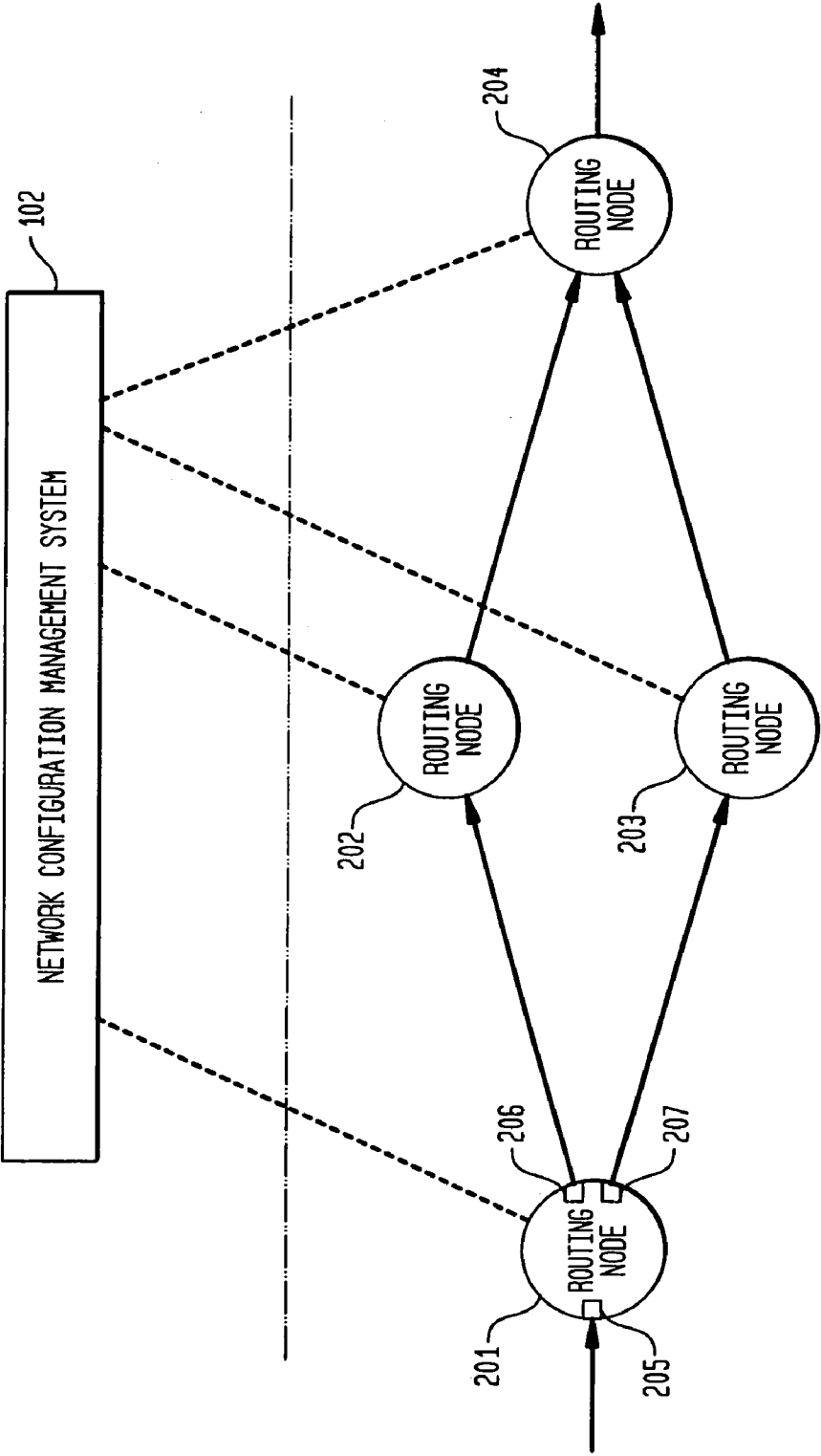


FIG. 1  
(Prior Art)



FIG. 2





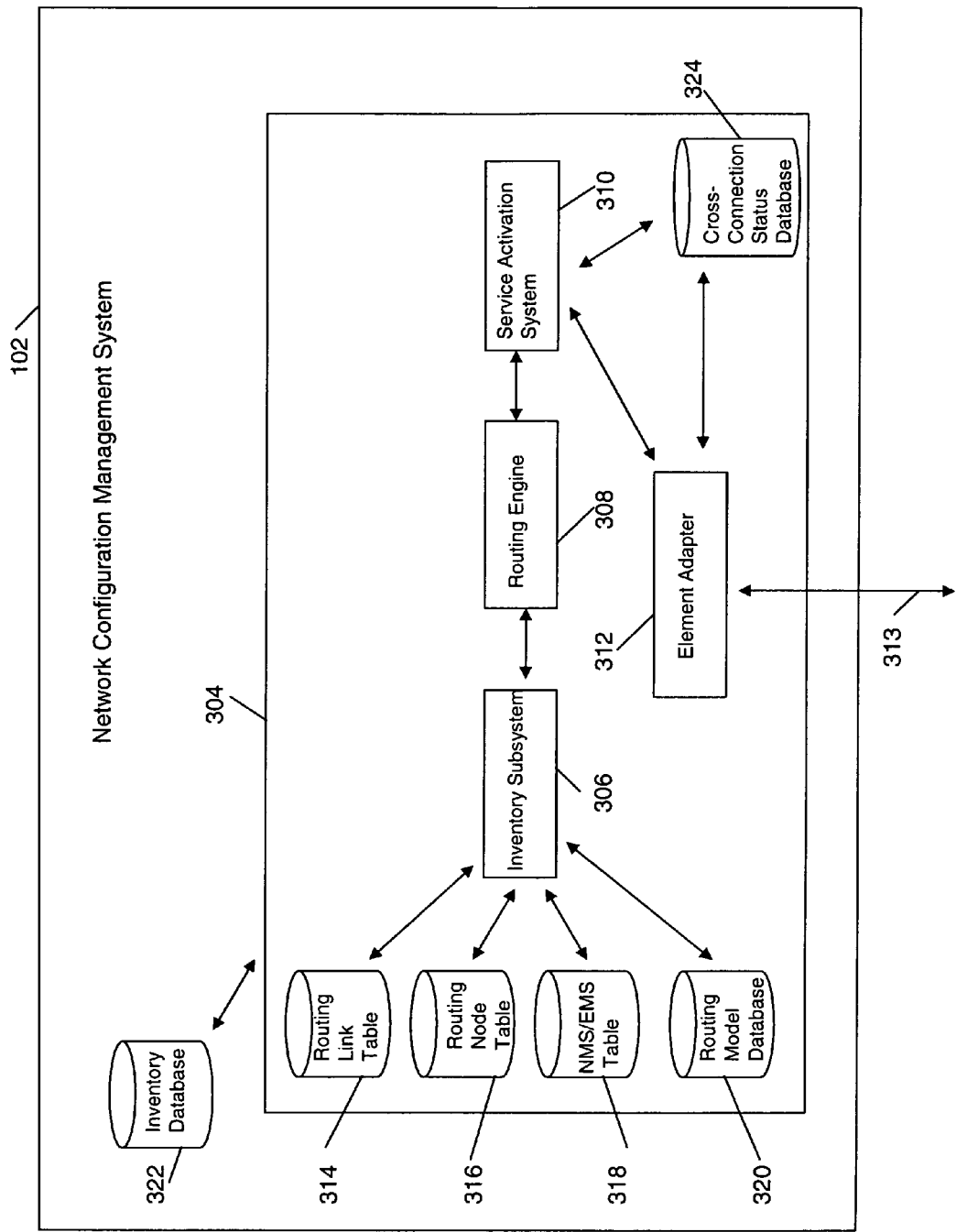


FIG. 3

FIG. 4

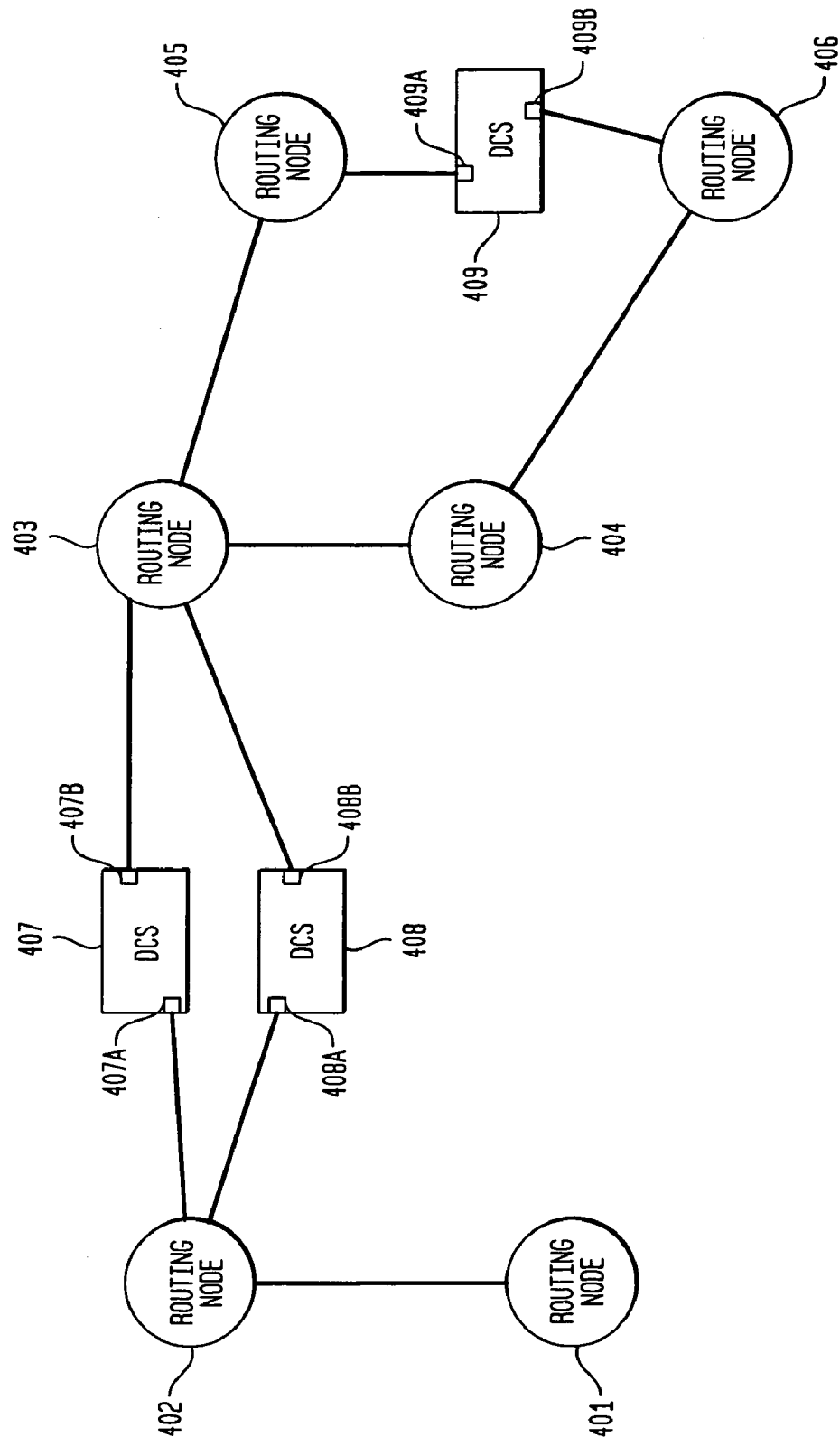
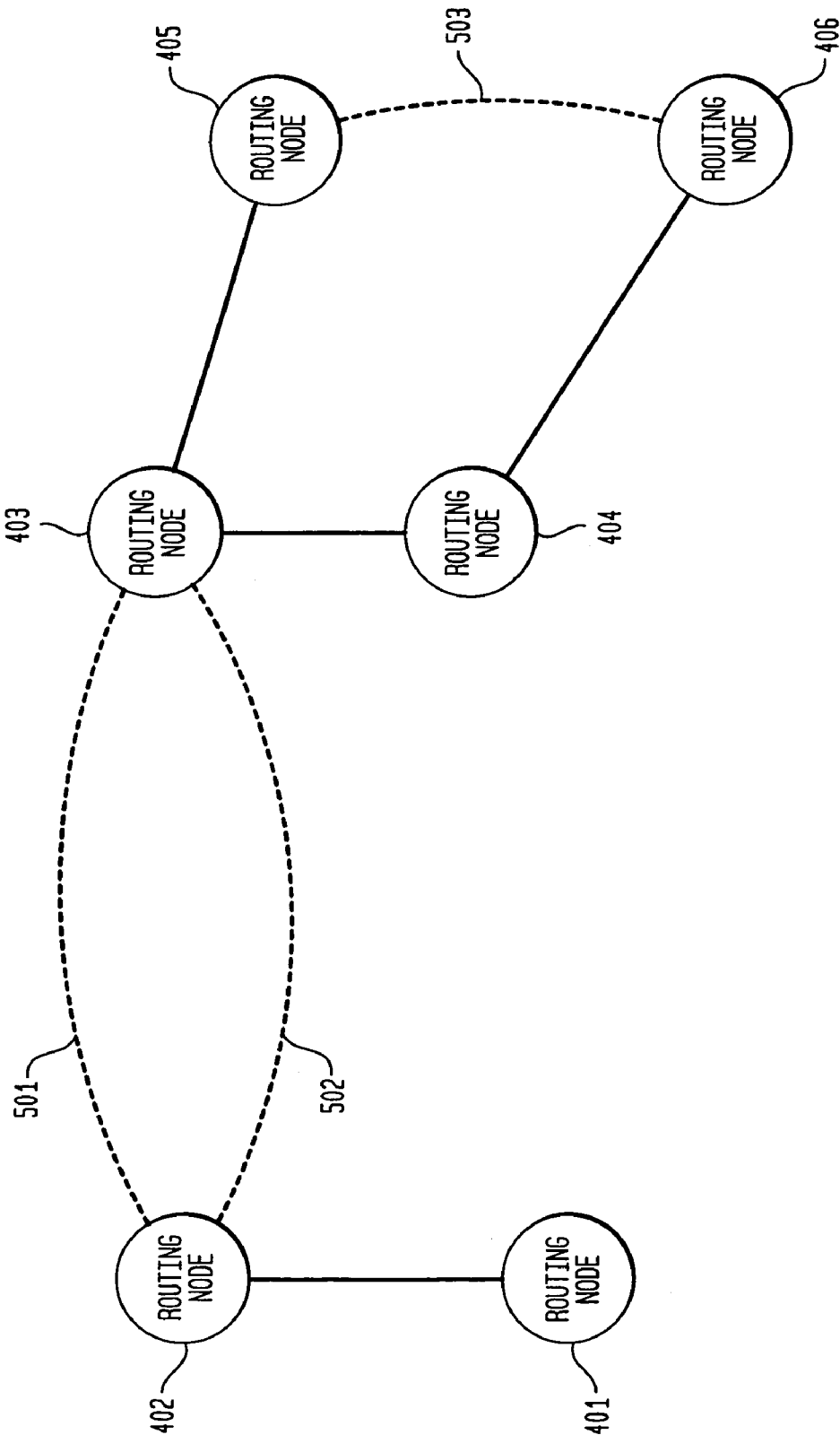


FIG. 5



US 7,760,664 B2

1

## DETERMINING AND PROVISIONING PATHS IN A NETWORK

This application claims the benefit of U.S. Provisional Application No. 60/614,609, filed Sep. 30, 2004, which is hereby incorporated herein by reference.

### BACKGROUND OF THE INVENTION

Communications networks, such as next generation broadband networks, have become increasingly complex due to increased size, numerous intermixed technologies/protocols (e.g., ATM, Frame Relay, etc.), and the intermixing of equipment manufactured by numerous different vendors. As a result, network configuration management systems that can provision virtual trunks and circuits within these networks are becoming increasingly important. Such network configuration management systems function to determine the paths/routes between network equipment, herein referred to as network elements, and to communicate with those network elements to realize desired trunks or circuits that facilitate the transmission of traffic across the network.

In general, network configuration management systems have traditionally determined the paths available by modeling portions of network elements as nodes on a graph and the links/interconnections between these portions as links between the nodes. More particularly, prior systems typically modeled every port of every network element as a node on the graph and modeled every physical link that interconnected these ports to one another as links that interconnected the nodes of the graph. The network model was then used to provision virtual trunks, which formed paths between network elements in the network. Once these virtual trunks were provisioned, virtual circuits could then be established across these trunks to support traffic flow from one point to another in the network.

FIG. 1 shows an exemplary prior art network configuration management system 102 and a network 110 managed by system 102. The network configuration management system 102 functions to determine a preferred path between two points in a network (i.e., between two network elements) and for provisioning a communications connection across this path by communicating with the managed network 110. Managed network 110 consists primarily of broadband network 112 which, in turn, consists of a plurality of network elements 114-118 interconnected by physical links and virtual trunks and circuits represented in FIG. 1 by links 120-124. The network elements comprise varying technologies and protocols and may be manufactured by different vendors. Managed network 110 further comprises network management systems, such as network management system (NMS) 126, and element management systems, such as element management system (EMS) 128. These systems are typically provided by the network element manufacturers and typically function to perform the actual configuration and management of the individual network elements.

NMSs and EMSs may function to control both the network elements and the links between those elements. However some may not control the links between the elements and, instead, only manage the network elements themselves. For example, an NMS, such as NMS 126, may function to collectively manage a set of network elements 114 and the physical links 120 between them, thus forming a collectively managed sub-network having network elements 114. Accordingly, when network traffic arrives at an ingress port into one of the network elements 114, such as port 130, the NMS 126 determines a set of links and network element

2

cross-connects to interconnect port 130 to an egress port, such as port 132. The NMS 126 then provisions the network elements to realize this interconnection. In another example, some management systems, such as EMS 128, may only manage one or more network elements 118, but not the links 124 between them. Here, a higher layer entity, such as the Network Configuration Management System 102, determines the links between network elements 118 required to create a path and then instructs the EMS to perform the necessary cross-connects within network elements 118 to realize the complete path.

FIG. 1 also shows how some network elements, such as network elements 116, are not managed by either an NMS or EMS. Specifically, a higher layer entity, once again such as Network Configuration Management System 102, directly communicates with these elements to perform network configuration functions. In this case, Network Configuration Management System 102 would configure any cross-connects within network elements 116 as well as any links between network elements. Thus, as shown in FIG. 1, to facilitate traffic flow across broadband network 112, for example from port 130 on network element 114 to network element 118, the combination of Network Configuration Management System 102, NMS 126 and EMS 128 will collectively determine an appropriate network path across and between network elements 114, 116 and then provision virtual trunks and circuits across network 112.

One difficulty with prior methods of using network configuration management systems, such as those described above, is that the modeling of the network elements, physical links, and virtual trunks and circuits results in very large, inefficient models that do not adapt well to diverse network elements and large networks. Specifically, such large models result in correspondingly large and complex network model graphs which, in turn, create performance and scalability issues due to the demanding processing requirements associated with such graphs. Therefore, in one prior attempt at solving this problem and to reduce the aforementioned disadvantages, a network model was created based on how the ingress and egress ports of each network element can be interconnected within themselves and to other network elements. Specifically, in this prior attempt, a simplified routing graph was created by the network configuration management system whereby, instead of modeling each port of a network element as a node on a routing graph, an entire network element itself could be represented as one or more routing nodes or, in some cases, multiple network elements could be represented as a single routing node. Referring to FIG. 2, for example, network elements 114 of FIG. 1 that are managed by NMS 126 are modeled as a single node 201. Additionally, network elements 118, which are managed by both EMS 128 and the Network Configuration Management System 102 are also modeled as a single routing node 204. Network elements 116 are each modeled as individual routing nodes, since the Network Configuration Management System 102 manages both the network element and the link between the elements. In such a model, therefore, the individual physical hardware links are not each modeled but, rather, one or more network elements are modeled as a single routing node based on how those network elements and the links between them are managed. Such an attempt is generally described in pending U.S. patent application Ser. No. 10/118,187, filed Apr. 8, 2002 and entitled "Determining and Provisioning Paths Within a Net-

US 7,760,664 B2

3

work of Communication Elements” (hereinafter referred to as the “’187 application”), which is hereby incorporated by reference herein in its entirety.

### SUMMARY OF THE INVENTION

While the prior methods of creating network models for routing traffic across networks and between multiple networks are advantageous in many regards, as discussed above they are limited in certain regards. In particular, while processing associated with network routing can be greatly simplified using the prior methods, such processing can still be resource and overhead intensive. This is especially the case as networks using different speeds and/or protocols are being interconnected to provide new and more complex services to customers.

Accordingly, the present inventor has invented a network provisioning system for establishing a path between two networks wherein a common network device between those networks is modeled as a link between a first network element in one network and a second network element in a second network. In one embodiment, a network routing graph is created by an inventory subsystem in a routing manager by inventorying the physical network elements and links in the network. The inventory subsystem then models those elements/links as a plurality of virtual nodes and links between the nodes. At least one common network device, such as a digital cross connect located at a junction between the two networks, is modeled as a link instead of a node. A routing engine then uses the network routing graph, including the link modeled from the common network device, to provision a path between the two networks. Thus, since fewer nodes are represented in a network graph of the modeled network, route processing is reduced, resulting in a corresponding reduction in overhead and resources required to route network traffic from one node to another.

### DESCRIPTION OF THE DRAWING

FIG. 1 shows a prior art managed broadband network and a network configuration management system for determining and provisioning routing paths within the network;

FIG. 2 shows a network routing model whereby some network elements are combined and treated as single routing nodes;

FIG. 3 shows an illustrative network configuration management system;

FIG. 4 shows a network routing model whereby Digital Cross Connect Systems (DCSs) are used to interconnect different network nodes; and

FIG. 5 shows a network routing model in accordance with the principles of the present invention whereby DCSs are modeled as links.

### DETAILED DESCRIPTION OF THE INVENTION

FIG. 3 shows an illustrative network configuration management system, such as Network Configuration Management System (NCMS) 102 in FIGS. 1 and 2. As discussed above, NCMS 102 determines preferred routing paths between two ports within the network by modeling the network paths as a plurality of routing nodes and links between the nodes, and for using these paths to provision virtual trunks and circuits within the networks. To accomplish this function, NCMS 102 includes, among other components, a routing manager 304 and inventory database 322. The routing manager 304 provides end-to-end connection management func-

4

tions including the determination and provisioning of routing paths in broadband network 112 in FIG. 1. In order to accomplish these functions, routing manager 304 comprises an inventory subsystem 306, a routing engine 308 and a service activation system 310. The routing manager 304 is connected to the various network elements via an element adapter 312 and connection 313. Broadly, the routing manager 304 maintains a topological graph comprising nodes and links that model the broadband network 112. This graph is used to determine and provision routing paths between, for example, two ports within the network. These paths are then used to provision virtual trunks and circuits.

The inventory subsystem 306 builds and maintains the topological graph in accordance with modeling methods such as those described above in association with the ’187 application. This graph is maintained, illustratively, in three database tables: routing link table 314, routing node table 316, and NMS/EMS table 318. The routing engine 308 determines a routing path for traffic through the network using the network graph maintained by the inventory subsystem 306. The service activation system 310 then uses the determined routing path to provision the actual virtual trunk or virtual circuit. Specifically, the service activation system 310 activates the routing engine 308 to obtain a routing path given two endpoints and then invokes the element adapter 312 which interfaces with network elements, NMSs and EMSs to physically provision the determined path. As such, the element adapter 312 functions as an interface between the routing manager 304 and the NMSs 126, EMSs 128, and network elements 116 in managed broadband network 112. As one skilled in the art will recognize, there is typically a specific element adapter designed for use with NMSs, EMSs, and network elements manufactured by different manufacturers. As such, a network management system may have multiple element adapters, or different modules in one element adapter. Accordingly, once the service activation system determines a routing path, it invokes the appropriate adapter(s) or adapter module(s) to communicate the required configuration settings to the management systems/elements 126, 128, and 116 to provision the determined path.

As one skilled in the art will recognize, and as is further discussed herein below, network traffic may be required to traverse multiple separate networks. These different networks may be interconnected with cross connects, such as digital cross connects (DCSs). As such, it is necessary for the NCMS 102 to also have available configuration and status information related to these DCSs. This configuration and status information is, illustratively, maintained in cross-connection status database 324. Thus, in provisioning the aforementioned path, service activation system 310 may also refer to cross-connection status database 324.

The prior illustrative method described in the ’187 application for using an NMS to simplify routing graphs is advantageous in many regards. By eliminating the need to inventory individual ports and by reducing the number of nodes necessary to consider in routing network traffic from one point to another, the processing overhead and timeliness associated with making routing decisions is greatly reduced. Additionally, such an approach adds considerable flexibility in designing and maintaining routing graphs. Specifically, as described in that application, instead of inventorying and maintaining a database of each port in a network and the interconnections between those ports, it is only necessary to inventory the routing nodes and the links between the routing nodes that, for example, may consist of several network elements.

As one skilled in the art will recognize, the method described in the ’187 application is primarily focused on

US 7,760,664 B2

5

network routing at layer 2 of the network. As is well understood, networks have been modeled as operating at different layers. One model for such network layers is known as the Open System Interconnection (OSI) model, which generally defines 7 different layers in the network. Layer 2 is also known as the data link layer and is the layer at which the physical medium is shared and where data link and media access are controlled. For example, in Ethernet networks, layer 2 is the layer at which network routing between media access control (MAC) addresses of individual hardware components is performed.

The above-described network model at layer 2 of a network is primarily useful within a single network. However, with increasingly complex and large networks it has become necessary to cross network boundaries in order to route network traffic from one destination to another. In many cases, the different networks rely on different protocols, operate at different speeds and may even operate using a different physical medium (e.g., copper vs. optical fiber). In order to interconnect such networks, DCSs or other similar devices, such as optical cross connect systems (OCSs), are used. As used herein, a DCS is any device that interconnects networks to facilitate traffic routing from one network to another or to link portions of networks using one protocol or traffic rate to another portion using a different protocol or rate. Such DCSs are very well known in the art and serve to efficiently manage disparate traffic protocols and line speeds in telecommunications system central offices as well as remote field locations and other locations such as within hotels and even at user premises. Such DCSs may be used in a variety of different applications. For example, DCSs may be used at a customer premises to interface with both voice protocol networks and a number of different data protocol networks in order to aggregate and cross connect these networks to a high-speed copper wire or optical fiber loop. Additionally, DCSs may be used in a digital loop carrier (DLC) capacity to aggregate networks using multiple protocols for transmission across a SONET ring network. In another common implementation, such DCSs may be used within, illustratively, a telecommunications central office in order to manage and cross connect channels from multiple SONET rings that are employed in an access network and/or a metro or inter-office network. Other uses of DCS are well known and will be obvious to one skilled in the art.

FIG. 4 shows one illustrative routing map wherein DCSs are used to connect networks to facilitate traffic flow from one network to another. In particular, FIG. 4 shows routing nodes 401-406, each of which represents, illustratively, a network, such as broadband network 112, or a portion of a network, such as the group of network elements 116 also in FIG. 1. As such, each of the routing nodes 401-406 illustratively has a plurality of network elements that are modeled, for routing purposes, as a single routing node with an ingress port and an egress port, such as ports 130 and 134, respectively, in FIG. 1. The networks represented by each of routing nodes 401-406 may, for example, operate using a different protocol or speed and, therefore, DCSs, such as DCSs 407, 408 and 409, may be used to aggregate and/or disaggregate traffic in order to facilitate the transmission of that traffic between and over the different networks interconnected by the DCSs. For example, routing nodes 402 and 405 may represent well-known OC-3 networks operating at an illustrative speed of 155.52 Mb/s while the networks represented by nodes 403 and 406 may be well-known OC-12 networks operating at an illustrative 622.08 Mb/s rate. DCSs 407 and 408 aggregate and/or disaggregate the data between the networks represented by nodes 402 and 403 and DCS 409 aggregates and disaggregates the

6

traffic between the networks represented by nodes 405 and 406. Typically, paths through DCSs 407-409 are provisioned in a relatively static manner. For example, a path from port 407A, associated with node 402, to port 407B, associated with node 403, is provisioned on DCS 407 in order to provide connectivity between the networks represented by nodes 402 and 403. Connections between ports 408A/408B and 409A/409B are similarly provisioned to connect nodes 402/403 and 405/406, respectively. Thus, one skilled in the art will recognize that DCSs 407-409 function as common nodes between the respective networks.

As one skilled in the art will recognize, a DCS, such as any one of DCSs 407-409, functions similarly in some respects to a network switch, such as a router or ATM switch. However, such routers/switches typically operate as a function at least in part of the signaling accompanying traffic transiting the network and, hence, such routers/switches are typically closely tied to specific services provided by a network service provider. A DCS is typically not used for such purposes. Instead, a DCS is typically used for transmission management at a higher level of the network. Specifically, unlike most telecom services where switch control is an inherent element of the service provided to customers and is closely tied to the protocol used at layer 2 of the network, DCSs are typically used as an engineering and provisioning control mechanism at layer 1 in the network (i.e., the physical layer of the network). As such, DCSs are typically not used to dynamically alter switching over a short time period, as are routers and other types of switches. Additionally, DCSs are not typically controlled as a function of signaling from a customer but are, instead, controlled directly by, for example, engineers at the service provider. Also unlike simpler network switches, a typical DCS facilitates the provisioning of network paths and connections across the DCS that are typically constant over a period of hours to months.

As service providers, such as telecommunication service providers, strive to provide more advanced features to consumers, interconnections and junctions between networks, such as those created by DCSs 407-409 and other similar devices, become greater in number and grow in importance. These interconnection devices must be taken into account when developing a network routing strategy. Traditionally, in making routing decisions, the network configuration management system modeled devices such as DCSs as one or more separate routing nodes. The present inventor have discovered, however, that such a modeling of DCSs increases the routing processing required due to a larger number of "hops" necessary to traverse nodes in the routing model. This increases both the time and overhead necessary to, for example, generate the aforementioned routing graphs. Therefore, the present inventor have further discovered that, in addition to simplifying routing decisions at layer 2 of a network, as described in the '187 application, it is desirable to also simplify the routing graph at layer 1 of the network. Specifically, instead of treating DCSs as a separate node (or multiple nodes corresponding the ports on the DCS) in the network, it is also desirable to model DCSs differently in order to further simplify the routing graphs/decisions. More particularly, in part since DCSs and other similar devices are relatively static in configuration, the present inventor have discovered that such devices may be treated as links, such as would be formed by a physical cable, instead of nodes that require processing as an affirmative routing hop.

As described above in association with the '187 application, prior to provisioning network paths in a network, such as network 112 in FIG. 1, a network configuration management system, such as NCMS 126 in FIG. 1 will inventory the



US 7,760,664 B2

7

network elements and links in the network. Once these elements and links are defined, the NCMS generates a routing graph showing the network topology in terms of routing nodes and links to be used in provisioning trunks/circuits across the network. FIG. 5 is a simplified representation of such a routing map. In particular, routing nodes 401-406 are as described above in association with FIG. 4. Each of those routing nodes consists, for example, of a plurality of network elements that are modeled at a high level as a single routing node in order to decrease the processing overhead required to provision the aforementioned trunks/circuits. However, instead of modeling the ports of DCSs 407-409 of FIG. 4 as individual nodes, or as multiple nodes, those illustrative DCSs are modeled as links 501, 502 and 503. Links 501, 502 and 503 are used in the routing graph of FIG. 5 to represent DCSs 407, 408 and 409, respectively. Accordingly, in accordance with the principles of the present invention, a cross-connect, such as a DCS, is not modeled as one or more routing nodes having various links connecting ports to each other and to external ports on other network elements. Instead, such a cross-connect is modeled as a separate link between network elements in one or more networks. Accordingly, the routing map is greatly simplified.

One skilled in the art will recognize that, as DCSs or other network components are added or deleted, the NCMS will inventory the network elements and links between the elements, treating DCSs as links as described above. Specifically, this inventory is conducted by the inventory subsystem 306 of FIG. 3. As a part of this inventory, routing link table 314, routing node table 316, NMS/EMS table 318 and cross connection status database 324 are updated with information about the links, nodes and cross connections in and between the networks managed by the NCMS 102. Therefore, in this inventory, information concerning each DCS will be updated in the cross-connection status database and those same DCSs will be updated as links in the routing link table. As a result, when service activation system 310 invokes the routing engine 308 to provision a path, that engine will treat the DCSs as links to be provisioned and not one or more network nodes corresponding to the ports on the DCS. When network traffic traverses a particular DCS, configuration and status information related to that DCS is retrieved from cross connection status database 324 to identify how the path across the DCS should be provisioned to route the traffic to the appropriate destination.

One skilled in the art will recognize that many variations are possible and that any or all of these embodiments described herein above may be combined in order to create a border element function that is decentralized depending upon the needs of a particular network in order to add flexibility to network design and to reduce routing management overhead costs. The foregoing Detailed Description is to be understood as being in every respect illustrative and exemplary, but not restrictive, and the scope of the invention disclosed herein is not to be determined from the Detailed Description, but rather from the claims as interpreted according to the full breadth permitted by the patent laws. It is to be understood that the embodiments shown and described herein are only illustrative of the principles of the present invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention. Those skilled in the art could implement various other feature combinations without departing from the scope and spirit of the invention.

The invention claimed is:

1. A network provisioning system for establishing a path between at least a first network element and at least a second

8

network element, said at least a first network element and said at least a second network element being interconnected through a digital cross connect system, said system comprising:

- a routing manager computer comprising an inventory subsystem and a routing engine, wherein the inventory subsystem is configured to model each of said at least a first network element and said at least a second network element as one or more routing nodes in a graph, said graph comprising a plurality of routing nodes and a plurality of links interconnecting said plurality of routing nodes; and wherein the routing engine is configured to use said graph for determining a path between said at least a first network element and said at least a second network element, wherein the inventory subsystem models said digital cross connect system as a link between said at least a first network element and said at least a second network element; and
- a cross connection status database configured to store a status of each interconnection of said plurality of routing nodes, wherein the status indicates whether a cross-connection using said digital cross connect was successfully provisioned.

2. The network provisioning system of claim 1 wherein said at least a first network element is in a first network and said at least a second network element is in a second network.

3. The network of claim 1, wherein the digital cross connect system comprises a first port associated with the first network element and a second port associated with the second network element.

4. A routing manager for provisioning paths for network traffic between a plurality of network elements in one or more networks wherein at least a first digital cross connect system is disposed between a first network element in said plurality of network elements and a second network element in said plurality of network elements, said routing manager comprising:

- means for creating a graph of routing nodes and links, said routing nodes representing one or more network elements in said plurality of network elements and said links representing interconnections between said routing nodes;
- means for modeling said at least a first digital cross connect system as a link between those routing nodes representing said first network element and said second network element; and
- means for storing a status of each of said interconnections, wherein the status indicates whether a cross-connection using said digital cross connect system was successfully provisioned.

5. The routing manager of claim 4 wherein said first network element is an element in a first network and said second network element is an element in a second network.

6. The routing manager of claim 4, wherein the digital cross connect system comprises a first port associated with the first network element and a second port associated with the second network element.

7. A method for routing network traffic between a first network and a second network, each of said first and second networks comprising a plurality of network elements, said plurality of network elements connected by a digital cross connect, said method comprising the steps of:

- determining, with a network configuration management system, the interconnections created by said digital



US 7,760,664 B2

9

cross connect between at least two network elements in  
said plurality of network elements; and  
representing each of said interconnections as a link  
between said at least two network elements; and  
storing a status of each of said interconnections in a cross  
connection status database, wherein the status indicates  
whether a cross-connection using said digital cross connect  
was successfully provisioned.  
8. The method of claim 7 further comprising provisioning  
a path between said at least two network elements.  
9. A method for determining a path between a first network  
element in first network and a second network element in a  
second network, said first network connected to said second  
network via a digital cross connect system, each of said  
networks comprising a plurality of network elements and a  
plurality of network links, said method comprising the steps  
of:  
modeling, via a network configuration management system,  
said plurality of network elements in said first and  
second networks as one or more routing nodes;  
modeling said network links as routing links, said routing  
links interconnecting said routing nodes;  
modeling said digital cross connect system as a routing link  
connecting a first routing node in said first network to a  
second routing node in said second network; and  
storing a status of each interconnection of said routing  
nodes, wherein the status indicates whether a cross-  
connection using said digital cross connect system was  
successfully provisioned.  
10. The method of claim 9 further comprising:  
storing said routing links in a routing link table.

10

11. The method of claim 9 further comprising the step of:  
determining a network path between said first routing node  
and said second routing node using said routing link.  
12. The method of claim 11 further comprising the step of:  
provisioning said network path to interconnect a first net-  
work element in said first routing node with a second  
network element in said second routing node.  
13. The method of claim 9, wherein the digital cross connect  
system comprises a first port associated with the first  
network element and a second port associated with the second  
network element.  
14. A method for determining a path between a first net-  
work element in a first network and a second network element  
in a second network, said first network connected to said  
second network via a common network device, each of said  
networks comprising a plurality of network elements and a  
plurality of network links, said method comprising the steps  
of:  
modeling, via a network configuration management system,  
said plurality of network elements in said first and  
second networks as one or more routing nodes;  
modeling said network links as routing links, said routing  
links interconnecting said routing nodes;  
modeling said common network device as a routing link  
connecting a first routing node in said first network to a  
second routing node in said second network; and  
maintaining a status of said routing links, said status indi-  
cating whether a cross-connection using at least one of  
said routing links was successfully provisioned.

\* \* \* \* \*

# Exhibit M

---



US008116315B2

(12) **United States Patent**  
**Posey, Jr.**

(10) **Patent No.:** **US 8,116,315 B2**  
(45) **Date of Patent:** **\*Feb. 14, 2012**

(54) **SYSTEM AND METHOD FOR PACKET CLASSIFICATION**

(75) Inventor: **Nolan J. Posey, Jr.**, Allen, TX (US)

(73) Assignee: **YT Networks Capital, LLC**,  
Wilmington, DE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 615 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/471,149**

(22) Filed: **Jun. 20, 2006**

(65) **Prior Publication Data**

US 2006/0239288 A1 Oct. 26, 2006

**Related U.S. Application Data**

(63) Continuation of application No. 10/138,760, filed on May 3, 2002, now Pat. No. 7,184,444, which is a continuation-in-part of application No. 09/698,666, filed on Oct. 27, 2000, now Pat. No. 6,665,495.

(51) **Int. Cl.**

**H04L 12/28** (2006.01)  
**H04L 12/56** (2006.01)  
**H04L 1/00** (2006.01)  
**H04L 12/26** (2006.01)  
**H04L 12/54** (2006.01)  
**G06F 15/173** (2006.01)  
**G06F 15/16** (2006.01)

(52) **U.S. Cl.** ..... 370/395.31; 370/395.43; 370/392; 370/395.1; 370/252; 370/398; 370/422; 370/428; 709/224; 709/249

(58) **Field of Classification Search** ..... 370/395.31, 370/395.43, 392, 395, 252, 389, 393, 395.1, 370/398, 395.6, 422, 428; 709/224, 249

See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,253,248 A 10/1993 Dravida et al.

(Continued)

**FOREIGN PATENT DOCUMENTS**

EP 0849916 A2 6/1998

(Continued)

**OTHER PUBLICATIONS**

Borgonovo et al. Unslotted deflection routing in all-optical networks; Global Telecommunications Conference, 1993, including a Communication Theory Mini-Conference. Technical Program Conference Record, IEEE in Houston. GLOBECOM '93., IEEE, Nov. 29-Dec. 2, 1993.

(Continued)

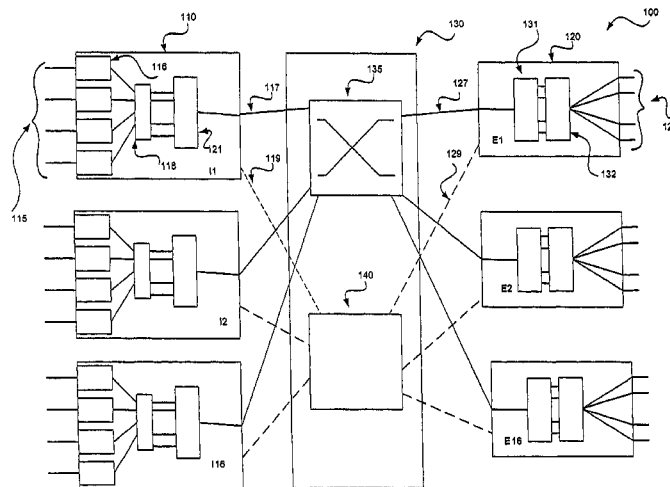
*Primary Examiner* — Ronald Abelson

(74) *Attorney, Agent, or Firm* — Connolly Bove Lodge & Hutz LLP

(57) **ABSTRACT**

The present invention provides method for data packet processing in a telecommunications system. The method of the present invention can include the steps of (i) determining a set of classification parameters for a data packet at an ingress edge unit, wherein the classification parameters include a packet destination, (ii) communicating the data packet to an egress edge unit and (iii) routing the data packet to a destination egress port at the egress edge unit according to the classification parameters determined at the ingress edge unit. In one embodiment of the present invention, the classification parameters can include a destination egress edge unit, a destination egress port at the destination egress edge unit, and quality of service parameter for proper processing of the data packet.

**21 Claims, 8 Drawing Sheets**



US 8,116,315 B2

Page 2

U.S. PATENT DOCUMENTS

5,303,078	A	4/1994	Brackett et al.	
5,327,552	A	7/1994	Liew	
5,351,146	A	9/1994	Chan et al.	
5,416,769	A	5/1995	Karol	
5,469,284	A	11/1995	Haas	
5,477,530	A	12/1995	Ahmadi et al.	
5,486,943	A	1/1996	Sasayama et al.	
5,546,391	A *	8/1996	Hochschild et al.	370/413
5,617,413	A	4/1997	Monacos	
5,734,486	A	3/1998	Guillemot et al.	
5,737,106	A	4/1998	Sansonetti et al.	
5,757,526	A	5/1998	Shiragaki et al.	
5,848,055	A	12/1998	Fedyk et al.	
5,978,359	A	11/1999	Caldara et al.	
6,005,698	A	12/1999	Huber et al.	
6,023,456	A	2/2000	Chapman	
6,052,726	A	4/2000	Fontenot	
6,320,858	B1 *	11/2001	King et al.	370/390
6,345,040	B1	2/2002	Stephens et al.	
6,501,869	B1	12/2002	Athale	
6,567,408	B1	5/2003	Lee	
6,674,754	B1	1/2004	Ofek	
6,721,315	B1	4/2004	Xiong et al.	
6,763,192	B1	7/2004	Jagannathan	
6,782,201	B2	8/2004	Yamamoto et al.	
6,819,870	B1	11/2004	Ge et al.	
6,834,310	B2	12/2004	Munger et al.	
6,859,579	B2	2/2005	Shiozawa et al.	
6,907,001	B1 *	6/2005	Nakayama et al.	370/230
6,928,244	B1	8/2005	Goldstein et al.	
6,975,638	B1 *	12/2005	Chen et al.	370/412
7,068,871	B2	6/2006	Sugama et al.	
2001/0043562	A1 *	11/2001	Hrastar et al.	370/227
2002/0015551	A1	2/2002	Tsuyama et al.	
2002/0048066	A1	4/2002	Antoniades et al.	
2002/0080446	A1	6/2002	Derventzis et al.	
2002/0101869	A1	8/2002	Garcia-Luna-Aceves	
2003/0030866	A1	2/2003	Yoo	
2003/0063348	A1	4/2003	Posey	
2003/0067653	A1	4/2003	Aicklen	
2004/0151171	A1	8/2004	Lee et al.	
2009/0067434	A1 *	3/2009	Brueckheimer et al.	370/395.1

FOREIGN PATENT DOCUMENTS

WO	WO 95/30318	A2	11/1995
WO	WO 00/42811	A1	7/2000

OTHER PUBLICATIONS

Chevalier et al. "A new packet routing strategy for ultra-fast photonic networks", Dept. of Electron & Electr. Eng., Strathclyde Univ., Glasgow; This paper appears in: Global Telecommunications Con-

ference, 1998, GLOBECOM '93., "The Bridge to Global Integratio", 1998.  
Bannister et al., "A performance model of deflection routing in multibuffer networks with non-uniform traffic Networking," IEEE/ACM Transactions on vol. 3, issue 5, pp. 509-520, Oct. 1995.  
Hunter, David K., "Buffering in optical packet switches", *Jrnl. Of Lightwave Technology*, vol. 16:12, pp. 2081-2094, Dec. 1998.  
Borgonovo et al. "On the design of optical deflection-routing networks", *INFOCOM '94. Networking for Global Communications. 13<sup>th</sup> Proceedings IEEE*, Publication Date: Jun. 12-16, 1994, pp. 120-129, vol. 1, Meeting Date: Jun. 12, 1194-Jun. 16, 1994.  
Li et al., "Deflection Routing in Slotted Self-Routing Networks with Arbitrary Topology," *IEEE Jrnl. On Selected Areas in Communications*, vol. 22:9, pp. 1812-1822, Nov. 2004.  
International Search Report for PCT/US01/51237, Mar. 20, 2003.  
Kanna, et al., "A High Bandwidth Space-Time-Wavelength Multiplexed Optical Switching Network", *Proceedings of the IEEE INFOCOM '97*, Los Alamitos, CA, Apr. 7-12, 1997.  
McKeown, et al., "Tiny Tera: A Packet Switch Core", IEEE Micro, IEEE Inc., New York, vol. 17, No. 1, pp. 26-33, Jan. 1997.  
Soeren Lykke Danielsen, et al., "WDM Packet Switch Architectures and Analysis of the Influence of Tuneable Wavelength Converters on the Performance", Jun. 1998.  
Soeren L. Danielsen, et al., IEEE Photonics Technology Letters, vol. 10, No. 6, "Optical Packet Switched Network Layer Without Optical Buffers", unknown.  
John M. Senior, et al., SPIE—The International Society of Optical Engineering, *All-Optical Networking: Architecture, Control and Management Issues* vol. 3531, pp. 455-464, Nov. 3-5, 1998.  
M.C. Chia, et al., Part of SPIE Conference on All-Optical Networking: Architecture, Control and Management Issues, "Performance of Feedback and Feedforward Arrayed—Waveguide Gratings-Based Optical Packet Switches with WDM Inputs/Outputs", Nov. 1998.  
G. Depovere, et. al., Philips Research Laboratories, "A Flexible Cross-Connect Network Using Multiple Object Carriers" all pages, unknown.  
John M. Senior, et al., SPIE—The International Society for Optical Engineering, "All-Optical Networking 1999: Architecture, Control, and Management Issues" vol. 3843, pp. 111-119, Sep. 19-21, 1999.  
Jonathan S. Turner, *Journal of High Speed Networks* 8 (1999) 3-16  
IOS Press, "Terabit Burst Switching", pp. 3-16, 1999.  
Ken-ichi Sato, IEEE Journal on Selected Areas in Communications, vol. 12, No. 1, Jan. 1994 "Network Performance and Integrity Enhancement with Optical Path Layer Technologies", pp. 159-170, Jan. 1994.  
F. Callegati, et al., *Optical Fiber Technology* 4, 1996 "Architecture and Performance of a Broadcast and Select Photonic Switch", pp. 266-284, 1998.

\* cited by examiner

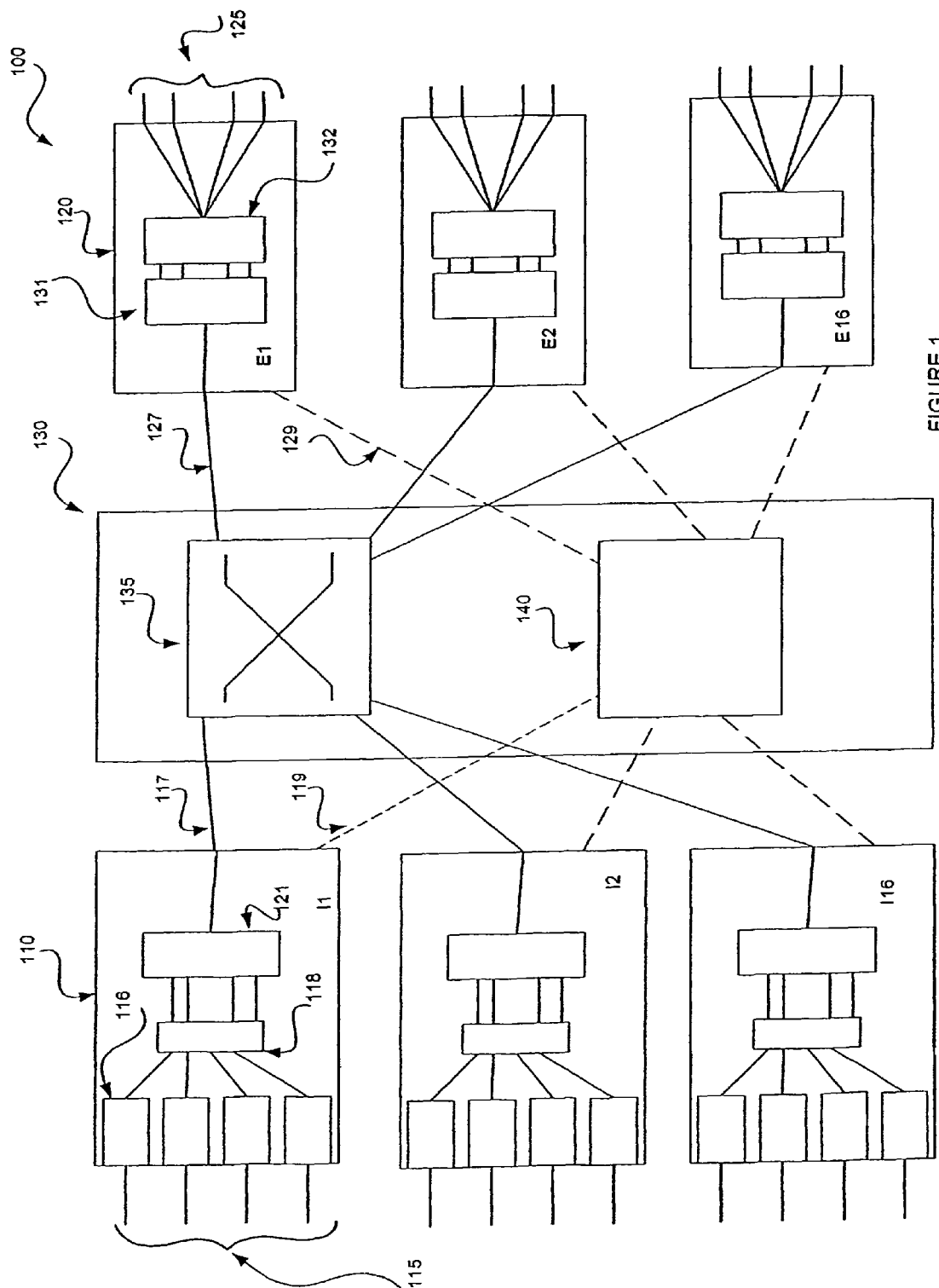
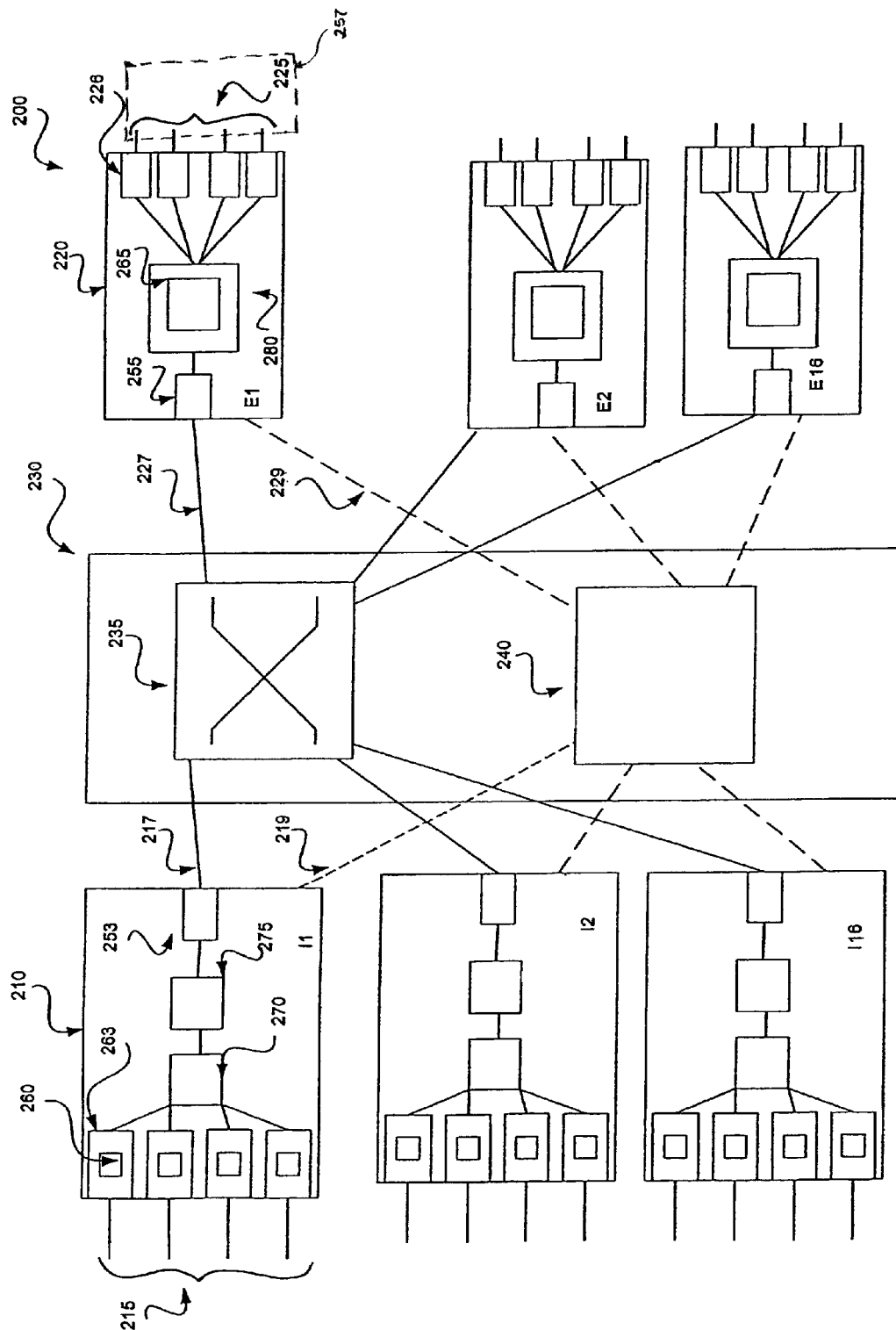
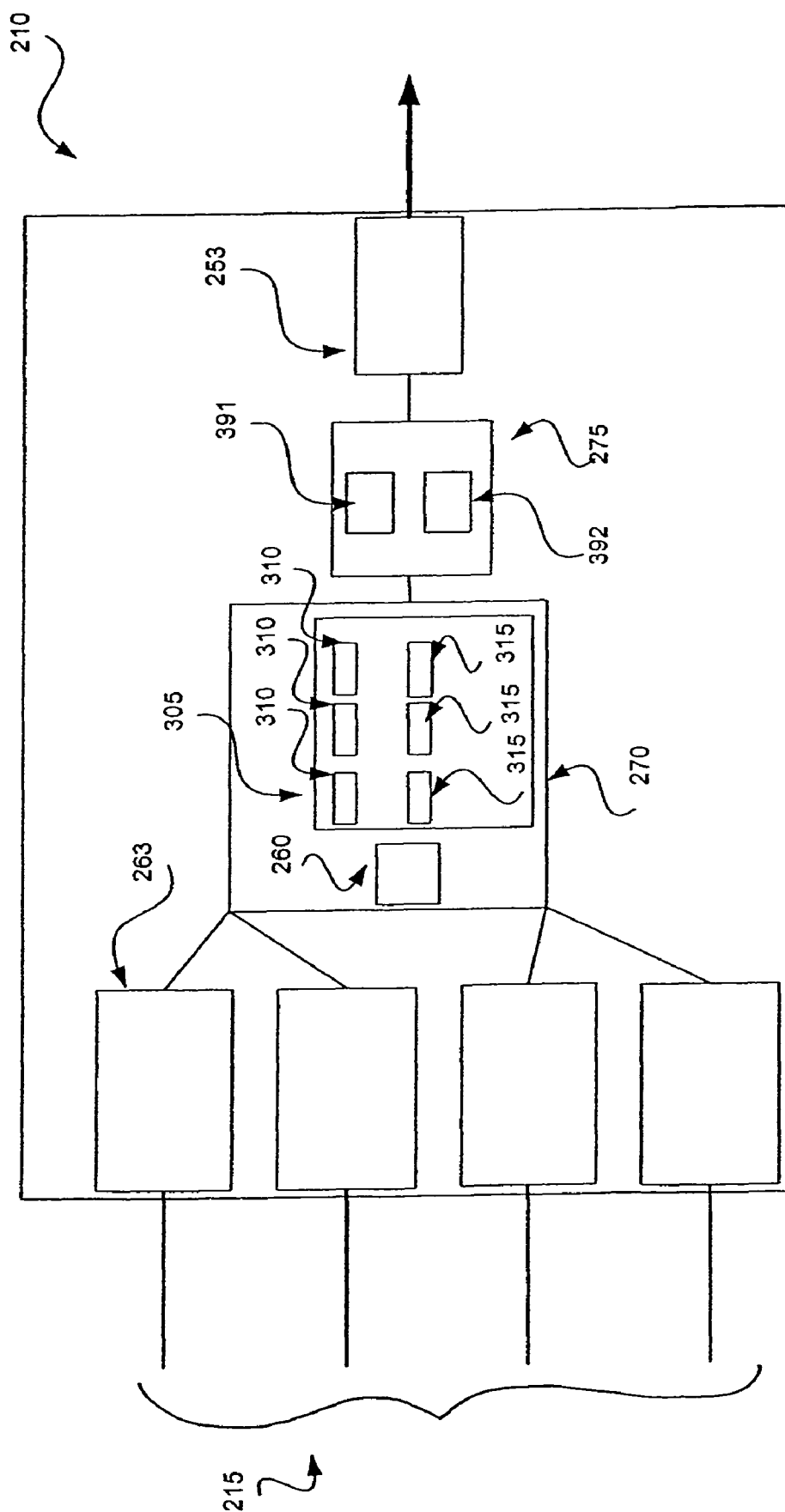


FIGURE 1



**FIGURE 2**





**FIGURE 3**

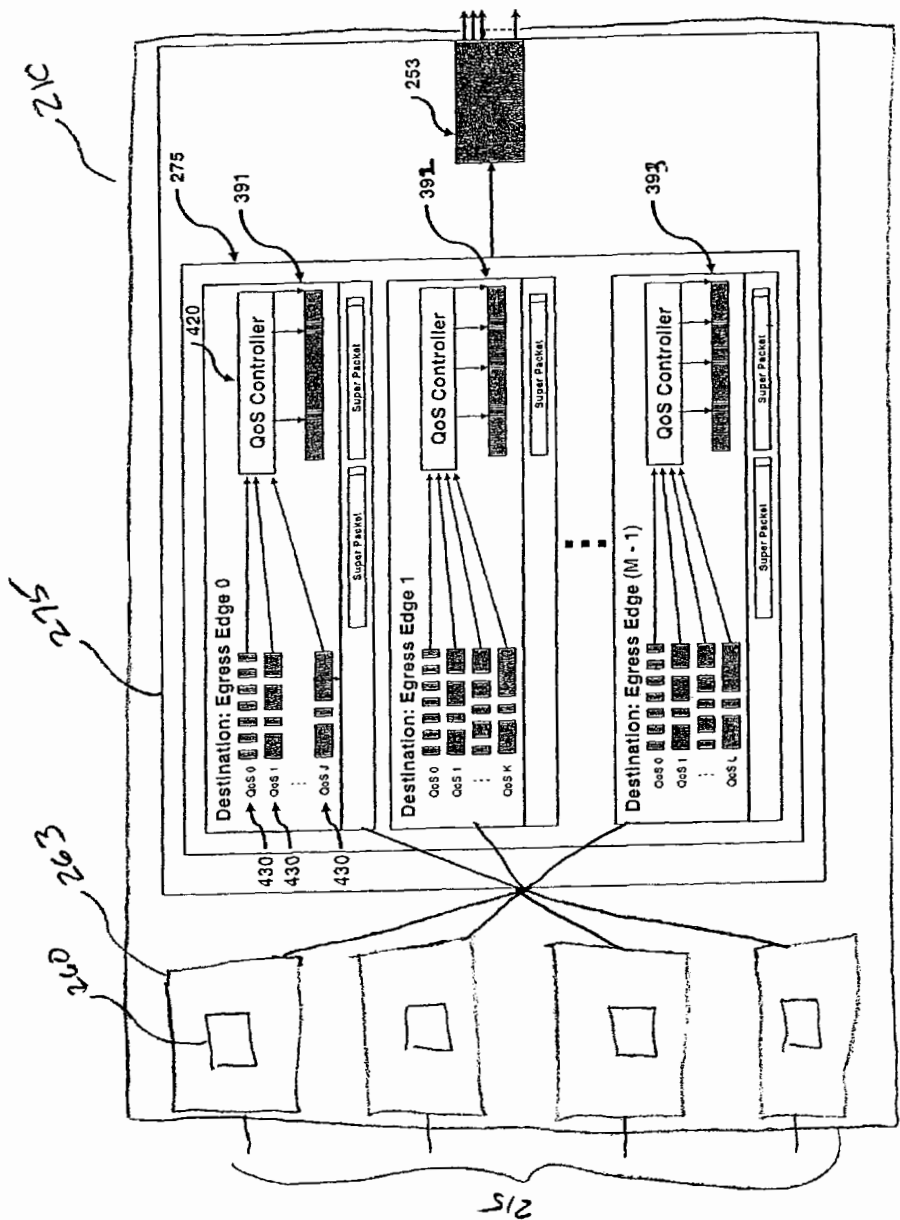


FIGURE 4

Figure 5A

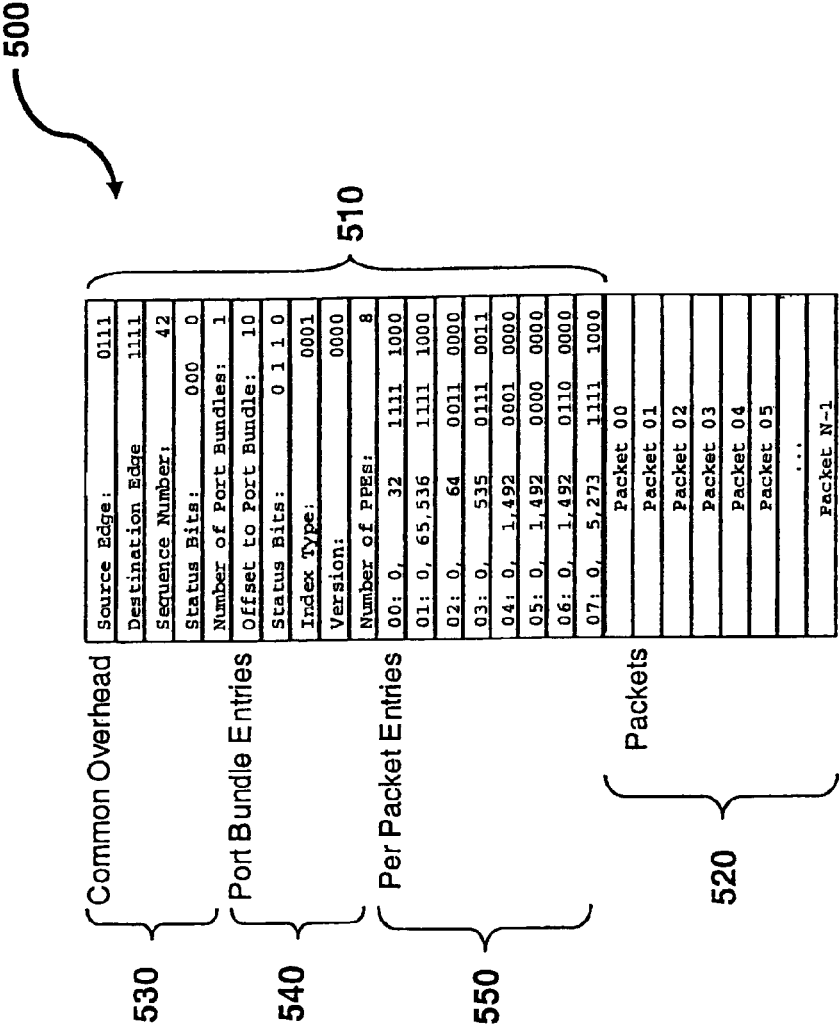


Figure 5B

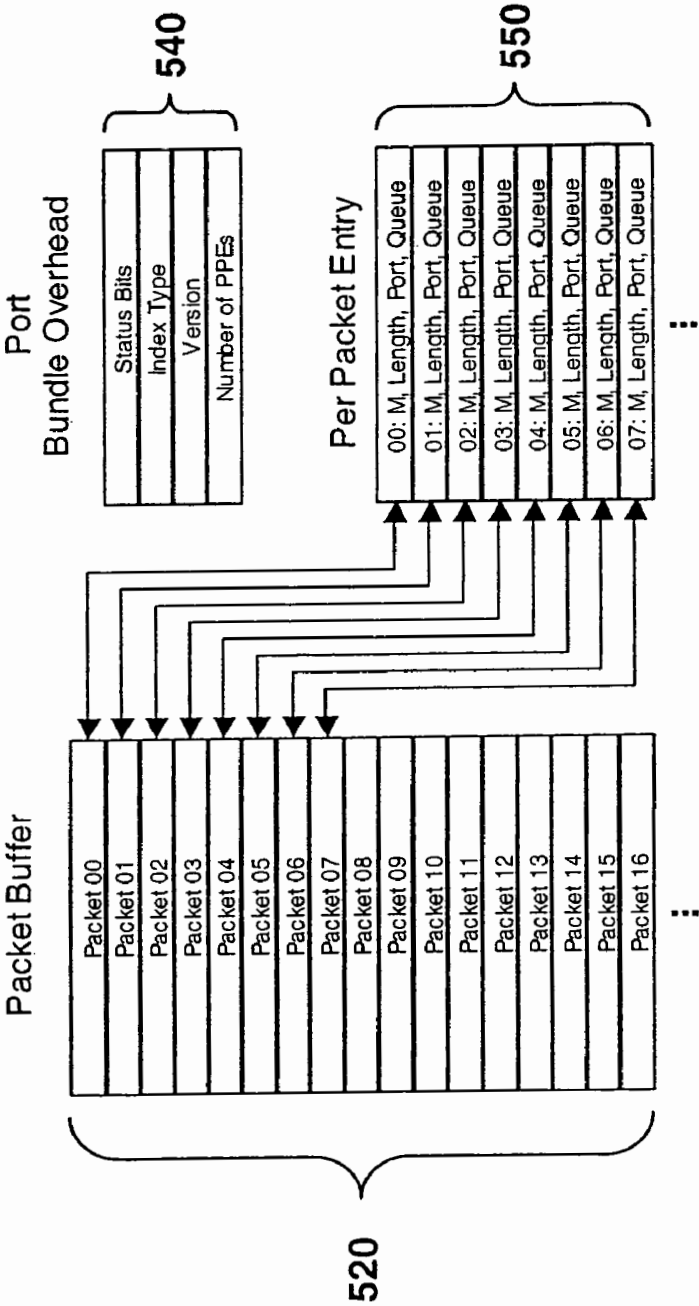


Figure 5C

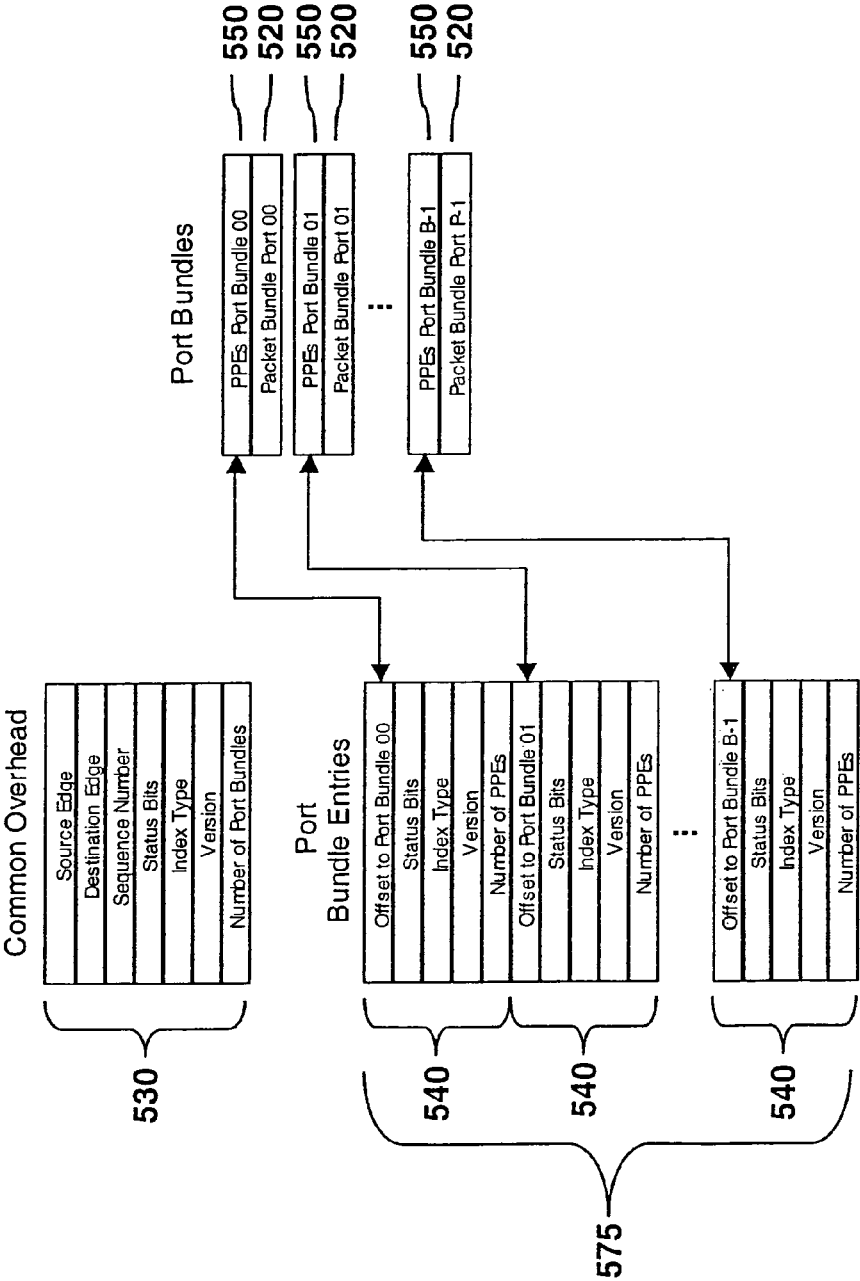
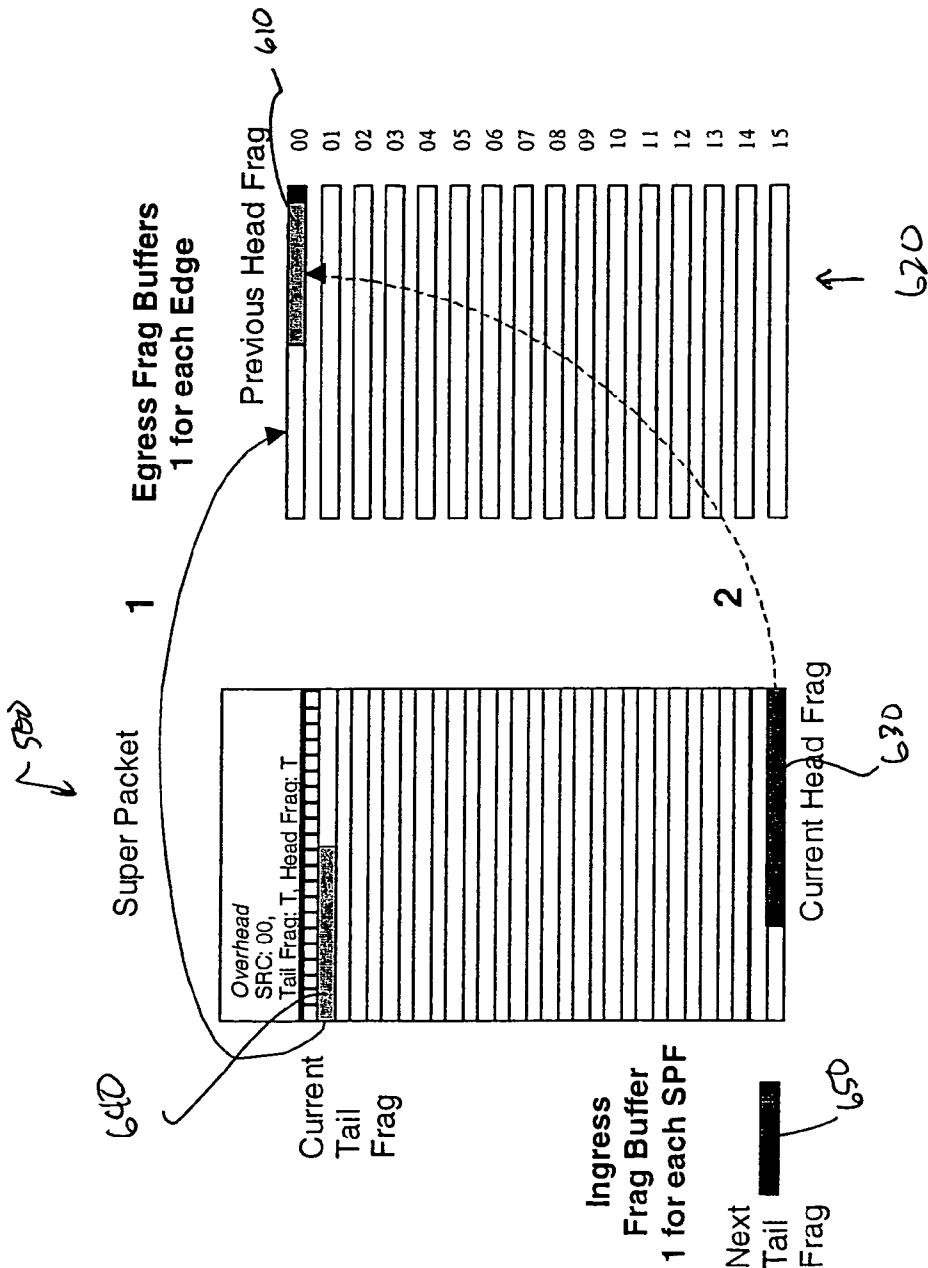


Figure 5D



US 8,116,315 B2

1

**SYSTEM AND METHOD FOR PACKET CLASSIFICATION**

## RELATED APPLICATIONS

This application is a continuation of and claims priority under 35 U.S.C. 120 from U.S. patent application Ser. No. 10,138,760, filed May 3, 2002, entitled "SYSTEM AND METHOD FOR PACKET CLASSIFICATION," now U.S. Pat. No. 7,184,444, which is a continuation-in-part of U.S. patent application Ser. No. 09/698,666, filed Oct. 27, 2000, entitled "Non-Blocking, Scalable Optical Router Architecture and Method for Routing Optical Traffic," now U.S. Pat. No. 6,665,495, both of which are hereby fully incorporated by reference.

## TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to telecommunications systems and methods, and more particularly, a system and method for classification of data packets to facilitate the routing of the data packets.

## BACKGROUND OF THE INVENTION

In telecommunications networks, routers and switches are used to direct data packets from a data packet's origin to its destination. Often a router or switch will have multiple incoming and outgoing transmission lines (or "ports"). Therefore, to route a packet through a telecommunications network, it is necessary to properly internally route the data packet at each router or switch from the incoming transmission port to the proper outgoing transmission port. This is commonly achieved by classifying the packets at the ingress edge of the switch/router. This classification of data packets can include determining the egress edge unit of the switch/router to which a particular data package should be routed. In this manner, data packets can be switched from a particular incoming transmission port to a particular outgoing transmission port through the switch/router.

In current data packet classification and routing systems, a data packet arrives at an ingress interface unit of a router where packet classification occurs. During packet classification, current systems will classify the data packet based on its destination port, which is associated with a particular egress edge unit. According to the classification, the router will route the data packet to the appropriate egress edge unit of the optical network for further routing. In current optical networks, however, the classification of a data packet is typically not retained once the data packet leaves the ingress edge unit in route to the egress edge unit.

In operation, data packets are classified in current systems and methods for classifying data packets based on the destination egress edge unit. When a packet arrives at the destination egress edge unit, classification is repeated to determine the destination egress interface port of the egress edge unit. Thus, the processing to determine the destination occurs in two stages. First it occurs at the ingress edge unit to determine to which egress edge unit a data package is bound and, again, at the egress edge unit to determine to which egress interface port the data package should be routed. Because classification occurs both at the ingress edge unit and the egress edge unit, current optical networks require that there be classification hardware at both units.

As noted, prior art packet classification systems and methods require repeating the classification process at the egress edge interface unit. Therefore, a need exists for a packet

2

classification system and a method that can perform the classification only at the ingress edge unit, thus reducing the complexity and computational requirements at the egress edge unit.

## SUMMARY OF THE INVENTION

The present invention provides a data packet classification system and method that substantially eliminates or reduces disadvantages and problems associated with previously developed data packet classification systems and methods used in telecommunications networks.

More specifically the present invention provides method for data packet classification in a telecommunications system. The method of the present invention can include the steps of (i) determining a set of classification parameters for a data packet at an ingress edge unit, wherein the classification parameters include a packet destination, (ii) communicating the data packet to an egress edge unit and (iii) routing the data packet to a destination egress port at the egress edge unit according to the classification parameters determined at the ingress edge unit. In one embodiment of the present invention, the classification parameters can include a destination egress edge unit, a destination egress port at the destination egress edge unit, and quality of service parameter for proper processing of the data packet.

The present invention provides substantial technical advantage over previously developed systems and methods for routing data packets because the present invention can route data packets to an egress port without reclassifying the data packet at the egress edge unit associated with the port, thus minimizing duplicative hardware and processing requirements at the egress edge unit.

The present invention provides another substantial advantage over previous systems and methods for routing data packets by eliminating the delay caused by reclassifying a data packet at an egress edge unit, thereby increasing the throughput of optical routers/switches utilizing the present invention.

The present invention provides yet another technical advantage by allowing the routing of multiple data packets to a single destination edge unit.

## BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

FIG. 1 is a diagrammatic representation of one embodiment of a router **100** that can perform data packet classification at the ingress edge unit according to the present invention;

FIG. 2 is a diagrammatic representation of a second embodiment of a router that can perform data packet classification according to the present invention;

FIG. 3 is a diagrammatic representation of one embodiment of an ingress edge unit that can perform packet classification according to the present invention;

FIG. 4 is a diagrammatic representation of a second embodiment of an ingress edge unit that can perform packet classification according to the present invention;

FIG. 5A illustrates one embodiment of super packet containing a classification index according to the present invention;



## US 8,116,315 B2

3

FIG. 5B illustrates one embodiment of a port bundle construction containing a classification index according to the present invention;

FIG. 5C illustrates one embodiment of a super packet construction containing a classification index according to the present invention; and

FIG. 5D illustrates one embodiment of combining fragments of packets from arriving super packets.

## DETAILED DESCRIPTION OF THE INVENTION

Preferred embodiments of the present invention are illustrated in the figures like numerals being used to refer to like and corresponding parts of the various drawings.

The invention provides a data packet classification system and method wherein a data packet can be classified at the ingress edge unit of a router/switch. The data packet can be routed to its destination egress interface port based on the classification parameters that were determined at the ingress edge unit of the router/switch. Because classification does not have to be repeated at the egress edge unit, duplicative processing and hardware requirements are substantially reduced.

FIG. 1 is a diagrammatic representation of one embodiment of a router 100 that can perform data packet classification at the ingress edge unit according to the present invention. Router 100 can include a number of ingress edge units 110 (shown in FIG. 1 as sixteen ingress edge units labeled 11, 12, 13 . . . 116), a number of egress edge units: (shown in FIG. 1 as sixteen egress edge units labeled E1, E2, E3 . . . E16) and an optical switch core 130 that comprises a switch fabric 135 and a controller 140. While each of the edge units is illustrated separately for the sake of simplicity, it should be understood that edge units comprising both an ingress edge unit and an egress edge unit in the same physical structure can be constructed. Each of the edge units 110 can communicate data to switch fabric 135 via ingress packet links 117 and each egress edge unit can receive data from switch fabric 135 via egress packet links 127. In one embodiment of the present invention the ingress packet links 117 and egress packet links 127 can be DWDM links. Additionally, each ingress edge unit and each egress edge unit can receive and communicate control information with controller 140 via ingress control links 119 and egress control links 129, respectively.

Each ingress edge unit 110 and each egress edge unit 120 of router 100 can include a variety of ingress interface ports 115 and egress interface ports 125, respectively, which can externally connect to an assortment of other network elements such as switches, routers, cross-connects and/or transmission equipment. The ingress interface ports 115 and egress interface ports 125 can support, for example, high bandwidth IP traffic and/or TDM traffic. In one embodiment of the present invention, each of these ports can support 10 Gbps and above.

In operation, data packets can arrive at an ingress edge unit 110 through the ingress interface ports 115. At each ingress interface port 115, an ingress port card 116 associated with an ingress interface port 115 can determine a set of classification parameters for an incoming data packet. In one embodiment, the classification parameters can include a destination egress edge unit and a destination egress interface port. Additionally, the classification parameters might include a quality of service ("QoS") parameter, including the type of service bits, source IP address, layer four and five classification, service level agreements, operator configuration and the QoS software in use. The classification parameters can be forwarded from each ingress port card 116 to controller 140 via ingress control links 119. Additionally, the classification parameters can be placed in a classification index for the data packet. The

4

classification index can be included in the overhead of the data packet sent to the egress edge unit.

Controller 140 can collect data from each ingress edge unit 110, egress edge unit 120 and switch fabric 135 on a periodic basis (e.g., every millisecond), create a schedule that effects each ingress edge unit 110 and egress edge unit 120 for the next cycle, and provide the schedule to each ingress edge unit 110 and each egress edge unit 120. During scheduling, controller 140 can use quality of service parameters to determine which of the arriving data packets should be sent at any given time or whether a data packet should be dropped (e.g., in a congestion situation). Algorithms such as random early detection, weighted random early detection, early packet discard and other algorithms could be used to determine which packets should be dropped. Based on this schedule, ingress port card 116 can place an incoming data packet in a QoS queue (for subsequent forwarding to TWDM converter 118) or forward the data directly to TWDM converter 118. Ingress port card 116 can maintain multiple QoS queues for each egress interface port 125.

At TWDM converter 118 data packets from each ingress interface port card 116 can be forwarded to wave slot ( $\mu\lambda$ ) buffers. There can be multiple  $\mu\lambda$  buffers for each ingress interface port 115, and the number of  $\mu\lambda$  buffers for each ingress interface port 115 can correspond to the number of egress interface ports 125 (e.g., if there are K egress interface ports there can be K  $\mu\lambda$  buffers for each ingress interface port). Data packets arriving at each ingress interface port 115 can be directed to the  $\mu\lambda$  buffer associated with the destination egress interface port 125 to which the data packet is bound. Thus, in one embodiment of the present invention, each  $\mu\lambda$  can contain data packets from the same ingress interface port 115 that are bound to the same egress interface port 125.

When the loading of the  $\mu\lambda$  buffers is complete for a cycle, the TWDM converter 118 can subdivide the available  $\mu\lambda$ s into as many channels as there are wavelengths utilized by the ingress packet links 117. It should be noted that each  $\mu\lambda$  can include zero data packets, a single data packet, or multiple data packets bound for the same egress interface port 125. DWDM transmitter 121 can then forward a  $\mu\lambda$  to optical switch fabric 135 for further routing to the destination egress edge unit. Each  $\mu\lambda$  can be forwarded across multiple data streams, one stream per lambda as supported by the DWDM lambda count.

As  $\mu\lambda$ s pass through optical switch fabric 135, controller 140 can control the configuration of switch fabric 135 so that each  $\mu\lambda$  is routed to the appropriate egress edge unit 120. Because controller 140 can dynamically reconfigure switch fabric 135 based on the schedule that it established, conflicts and contentions of  $\mu\lambda$ s in switch fabric 135 can be avoided. At each egress edge unit 120, a DWDM receiver 131 can receive various  $\mu\lambda$ s from switch fabric 135 that have been directed from each ingress edge unit 110 to the receiving egress edge unit 120. The DWDM receiver 131 can demultiplex each  $\mu\lambda$  and generate a separate optical stream for each wavelength that was present in the DWDM lambda count. Egress TWDM converter 132 can buffer each  $\mu\lambda$  received and route the  $\mu\lambda$ s to the destination egress port cards 126 according to the schedule received from controller 140. The egress output port cards 126 could then forward the data to external components in the optical network. Additionally, if a classification index was included in the overhead of the data packet, egress edge unit 120 can read the classification index to determine routing information, quality of service processing, etc. However, it should be noted that reading the classification index can be done with simplistic table reading hardware/software, and does not require that the data packet actually be reclassified at

## US 8,116,315 B2

5

egress edge unit **120**. The classification parameters are used to implement QoS handling in the egress ports **126**.

As can be understood from the foregoing discussion, ingress edge unit **110** can determine a set of classification parameters, which can include a destination egress edge unit, a destination egress port, and QoS parameters for each incoming data packet. These classification parameters can be used by controller **140** to schedule the transmission of data packets to the destination egress edge unit, and, additionally, the transmission of data packets within the destination egress edge unit to the destination egress interface port. Because the routing of a data packet to the egress edge port can be controlled externally to the egress edge unit based on classification parameter determined at the ingress edge unit, data packets do not have to be reclassified at the egress edge unit. Therefore, duplicative classification hardware and software can be eliminated.

The discussion accompanying FIG. **1** described an exemplary embodiment of router **100**. However, it should be understood that the present invention can be utilized to classify data packets at an ingress edge unit, without reclassification at the egress edge unit, in many configurations of optical routers or switches in an optical network.

FIG. **2** is a diagrammatic representation of a second embodiment of a router **200** that can perform data packet classification at the ingress edge unit according to the present invention. Router **200** can include one or more ingress edge units **210**, one or more egress edge units **220** and an optical switch core **230** for routing data packets between an ingress edge unit **210** and an egress edge unit **220** that can comprise an optical switch fabric **235** and a controller **240**. While, for the sake of simplicity, the ingress and egress edge units are shown separately in FIG. **2**, it should be understood the combined edge units can be constructed with an ingress edge unit and an egress edge unit in a single physical edge unit. Each ingress edge unit **210** and each egress edge unit **220** can contain many ingress and egress ports of different types, respectively, that can connect to a range of other optical network elements, such as switches, routers, cross-connects, and/or transmission equipment. Additionally, optical switch core **230** can comprise a single switch core or alternatively, can comprise a stack of switch cores or a multiple plane switch core.

For the sake of explanation, Router **200** could have **16** ingress edge units (labeled **I1, I2, I3 . . . I16**) and **16** egress edge units (labeled **E1, E2, E3 . . . E16**). Each edge unit could have **16 OC-192** ports that use packet over SONET to connect to other network elements. Each ingress edge unit **210** and each egress edge unit **220** can be connected to optical switch core **230** using WDM links with **16λ** (**16** ports) running at **10 Gbps** for an aggregate of **265 Gbps**. Each ingress edge unit can connect to switch fabric **235** via Ingress packet links **217** while Egress edge units can connect to switch fabric **235** via egress packet links **227**. Additionally, ingress and egress edge units can exchange control information with controller **240** via ingress control links **219** and egress control links **229**, respectively. The router illustrated in FIG. **2** is exemplary only and other router configurations, combinations of ingress and egress edge units, data rates and ports are possible. For a more detailed explanation of one embodiment of router **200** that can be used in conjunction with the present invention, see U.S. patent application Ser. No. **09/698,666**, entitled "A Non-blocking Scalable Optical Router Architecture and Method for Routing Optical Traffic," incorporated by reference in its entirety.

In one embodiment of the present invention, router **200** can receive data packets from an ingress interface port **215**. The

6

data packets can be routed through ingress edge unit **210** to optical switch core **230** via an ingress edge unit output port **253**. Egress edge unit **220** can receive data packets from the optical switch core **230** by egress edge unit input port **255**, and transmit the data packets to the optical network through egress interface ports **225**, which can be associated with an interface output card **257**. In one embodiment, the ingress edge unit output port **253** can be an output WDM port and the egress edge unit input port **255** can be an input WDM port. Each ingress edge unit **210** can include a classification index module **260** for classifying data packets and each egress edge unit **220** can include a classification index processing module **265** for processing a packet classification index provided by classification index module **260**. In one embodiment, the classification index module **260** can be contained in an ingress port card **263**, however, it should be understood that the classification index module **260** functionality can be contained in any number of other units of router **200**, such as at a super packet processor **270**.

In operation, the data packets can be received at ingress edge unit **210** where classification index module **260** can determine the classification parameters for the data packet by reading the destination of the data packet from each packet's data packet header. If the packet's destination is given in the form of an IP address or other forwarding information, classification index module **260** can access a destination look-up table contained on a database that is accessible by classification index module **260** to correlate the data packet destination IP address to a destination egress edge interface unit **220** and a destination egress edge unit port **225** at that destination egress edge unit **220**. Thus, classification index module **260** can determine for each data packet arriving at ingress edge unit **210** both the destination egress edge unit out of many egress edge units and a destination port within the destination egress edge unit out of many potential ports in the destination egress edge unit. In one embodiment of the present invention, the destination information, such as the egress edge unit and the egress interface port, can be placed in a classification index, which can be included in the overhead of the data packet. Alternatively, if super packets are being constructed by router **200**, data packets that have been classified by classification index module **260** can be forwarded to super packet processor **270** and super packet factory **275** for aggregation into super packets and the classification parameters for individual data packets can be included in the overhead for the super packet. The construction of super packets will be discussed in conjunction with FIGS. **3** and **4**.

The data packet (or super packet) with the classification index can then be sent to the appropriate egress edge unit **220** via optical switch core **230**. At egress edge unit **220**, classification index processing module **265** can read the egress edge unit destination port from the classification index and forward the data packet to the appropriate egress edge unit destination port; e.g., one of egress interface ports **225**. Additionally, if super packets were constructed, egress edge unit super packet factory **275** can disassemble the super packets so that constituent data packets can be routed to the appropriate destination egress interface port according to the classification index. Because the destination port of an isolated data packet or a data packet in a super packet can be represented in a classification index, classification index processing module **265** can consist of simplistic table processing hardware or software.

In addition to reading the destination egress edge unit and the destination egress unit port for an incoming packet, classification index module **260** can determine quality of service parameters for the incoming data packet, including the type of

US 8,116,315 B2

7

service bits, the source IP address, layer four and five classification, service level agreements, operator configuration and the QoS software in use. It should be understood that these quality of service parameters are exemplary only and any quality of service parameters could be part of a data packet classification; e.g., TDM traffic, etc. Additionally, classification index module 260 can read other parameters from the packet header, including HDLC/PDT, IPV4, IPV6, NTLS, unicast or multicast. Classification index module 260 can then create a quality of service parameter vector which can be a compression of the quality of service parameters into code points that require less space so that the transported data from the ingress edge unit 210 to the destination egress edge unit 220 includes only the address information and the quality of service parameters vector, thus saving bandwidth. The quality of service parameters from a data packet can be used by controller 240 to determine which data packet should be sent at any given time. Additionally, the quality of service parameters could be used to determine if a data packet should be dropped based on the number of data packets. Algorithms such as random early detection, weighted random early detection, early packet discard and other well known algorithms could be used to determine which packets should be dropped.

Along with QoS parameters, the classification index can include information about queue management. For each quality of service supported by a router 200, each ingress edge unit and egress edge unit could have a queue to buffer data for transport with a particular quality of service. Thus, if router 200 supported J qualities of service, ingress edge unit 210 and egress edge unit 220 could have J quality of service queues. The ingress edge unit queue and/or the egress edge unit queue can be included in the classification index. In this manner, data packets can be direct to the appropriate queue for transport with a particular quality of service.

When the classification index and data packet arrive at egress unit 220, classification index processing module 265 can read the classification index for the data packet and forward the data packet to the appropriate egress interface port 225. In one embodiment of the present invention, at the destination egress interface card 226, a second table reader can also read the classification index to determine the quality of service for a data packet and to determine how the packet gets processed.

Because the present invention allows data packets to be routed from an ingress edge unit to port at an egress edge unit without reclassification of the data packet, the egress edge unit duplication of processing steps is reduced. Additionally, as the classification index can be read at the egress edge unit by simple table reading hardware or software, the hardware requirements for the egress edge unit are similarly reduced.

In addition to routing individual packets from an ingress edge unit 210 to an egress interface port 225 at an egress edge unit 220 without reclassification of the packet at the egress edge unit 220, the present invention can route super packets between an ingress edge unit 210 and ports 225 of the egress edge unit 220 without reclassification of the individual data packets at the egress edge unit 220. FIG. 3 is a diagrammatic representation of one embodiment of an ingress edge unit 210 capable of constructing super packets. In operation, an individual data packet arrives at the ingress edge unit 210 via an ingress interface port 215 destined for an egress interface port 225 of an egress edge unit 220. Classification index module 260, in one embodiment of the present invention can be located at a super packet processor 270. Super packet processor 270 can determine the length of a packet and phase align the incoming packet to convert the incoming data from a serial format to a parallel format. Classification index module

8

260 can determine, from the packet headers of the optical data packets, the egress edge unit 220 to which an incoming data packet is bound, the egress port 225 at the destination egress edge unit to which the data packet is bound, and other routing information (e.g., quality of service parameters and whether the incoming data packet contains TDM data). Super packet processor 270 can then route TDM data to TDM queues 310 within the packet classification queues 305 while routing PKT data to PKT queues 315 within the classification queues 305. The packet classification queue 305 can be memory device containing individual queues (or buffers) for storing various portions of the incoming data packets. The number of TDM queues and PKT queues can be determined by the number of egress edge units available.

With reference to FIG. 1, there are sixteen egress edge units available so there should be sixteen TDM queues and sixteen PKT queues in each set of queues, with each TDM queue and each PKT queue within a set of queues being assigned to a different egress edge unit. Thus, the TDM queue 310 assigned to the first egress edge unit 220 can collect the TDM data from incoming packets intended for the first egress edge unit 220, while the PKT queue 315 assigned to the first egress edge unit 220 can collect PKT data from incoming packets intended for the first egress edge unit.

Because all of the TDM data intended for any particular egress edge unit 220 gets collected in one particular TDM queue 310 and all of the PKT data intended for a particular egress edge unit gets collected in a single PKT queue 315, each packet classification queue 305 begins the process of building super packets by building a "partial" super packet, or "port bundle", containing all of the data arriving at one specific network port. 215 that is destined for a particular egress edge unit 265. Information that is common to all the data packets in a port bundle can be extracted by super packet processor 270 and be placed into the overhead of the port bundle along with classification information relevant to individual data packets. Super packet processor 270 can then forward the port bundles to super packet factory 275 where a super packet sub factory can assemble port bundles destined for each egress edge unit into super packets. Because super packets can be assembled for each egress edge unit, each super packet factory 275 can contain one super packet sub factory for each egress edge unit. For example, super packet sub factory 391 could correspond to the first egress edge unit, while super packet sub factory 392 could correspond to the second egress edge unit, and so on. In addition to assembling super packets, a super packet sub factory can derive information that is pertinent to a super packet as a whole and include that information in a super packet's classification index along with classification information regarding port bundles and classification information regarding the individual data packets in the super packet.

FIG. 4, is a diagrammatic representation of an alternative embodiment of an ingress edge router that is capable of constructing super packets. As shown in FIG. 4, the QoS controller module 420 can build a classification index for each super packet that includes the classification parameters for each data packet. The classification index can be built so that each data packet has a classification entry in the classification index (e.g. a "per packet entry"). The classification index can be placed in the overhead of each super packet. The super packets, each with a classification index, can then be sent to an optical switch core 230 (not shown) to be routed to the appropriate destination egress edge unit 220. Thus, both the egress destination port processing and packet classification processing can occur at the packet classification module 260, and can be performed simultaneously. This essentially pushes



US 8,116,315 B2

9

the destination port determination function upstream from the egress edge to the ingress edge.

As shown in the embodiment of FIG. 4, the classification index module 260, which in this embodiment can be located at the input interface card 263, can forward the data to an ingress super packet factory 275 that will aggregate data intended for the same destination egress edge unit 220 into super packets. Each ingress super packet factory 275 can comprise a number of sub-factories (e.g., one sub-factory for each egress edge unit 265), where each sub-factory builds super packets destined for one of M destination egress edge units 220 (which can be individually designated E1, E2 . . . EM-1). Each egress edge unit 220 also has L destination output ports 225 (which can be individually designated P1, P2 . . . PL-1). Additionally, each egress edge unit 220 can have a different number of QoS parameters with a QoS parameter queue 430 for each QoS parameter. Thus, as shown in FIG. 4, ingress super packet factory 275 has different sub-factories 391, 392 and 393, where sub-factory 391 correlates to egress edge unit number one (e.g., E1) and has J number of QoS parameters and J QoS parameter queues, while sub-factory 392 corresponds to egress edge unit E2 and has K QoS parameters and sub-factory 393 corresponds to egress edge unit EM-1 and has L QoS parameters.

Ingress super packet factory 275 uses QoS controller 402 to build super packets for each of the M-1 egress edge units 220 by collecting all of the various data (having different QoS parameters) intended for the same destination egress edge unit 220. The QoS controller 420 builds the super packets from each of the various QoS parameter queues 430 in a particular sub-factory. After the super packets have been built, a port scheduler can forward the super packets from each of the ingress super packet factories 275, segment the super packets to place the data from the super packets onto all of the wavelengths over which it will be transported (e.g., in an ordered array) and transport the super packet across the multiple lambdas to an optical switch core (not shown).

It should be understood that the embodiments described in conjunction with FIGS. 3 and 4 are by way of example only, and a super packet could be constructed in many ways. However, for the purposes of the present invention, regardless of how a super packet is constructed each super packet can contain a classification index that classifies the data packets within the super packet so that the constituent data packets do not need to be reclassified at the destination egress edge unit.

FIG. 5A illustrates one embodiment of a super packet 500 containing a classification index 510 according to the present invention. Super packet 500 can contain aggregated data packets 520 and a packet classification index 510 that can include a common overhead 530, a port bundle entry 540 and per packet entries 550. The common overhead 530 can contain classification parameters that are common to all the port bundles in super packet 500, port bundle entry 540 can include classification parameters that are common to each of the data packets in a port bundle and the per packet entries 550 can contain classification information for the individual data packets in super packet 530. While only one port bundle is shown in FIG. 5A (e.g., there is only one port bundle entry 540) it should be understood that super packet 500 could contain several port bundles or no port bundles.

FIG. 5B illustrates one embodiment of a port bundle construction according to the present invention. Classification index module 260 can derive per packet classification information based on data extracted from the individual packet

10

headers for the data packets. Thus, for example, per packet entry "00" corresponds to the classification information for packet "00", per packet entry "01" corresponds to the classification information for packet "01", and so on. At super packet processor 270, data packets arriving at the same ingress interface port 215 that are destined for the same egress edge unit 220 can be aggregated together into port bundles. Super packet processor 270 can then extract information based on commonalities between all of the packets, including the formatting of the per packet information (e.g., the index type), the version of software or hardware used to process the data packets, the status bits, and the number of per packet entries. Thus, a particular port bundle can include packets that are destined for the same egress edge unit 220, per packet information 550 for each data packet, and port bundle information 540 which is common to all the data packets in the port bundle.

FIG. 5C illustrates one embodiment of a super packet construction according to the present invention. As illustrated in FIG. 5C, various port bundles 575 can be aggregated together. Thus, for example, port bundle "00" through port bundle N-1 can be bundled together into a super packet at a super packet sub factory. The port bundles can include the per packet entries 550 for each port bundle and the group of data packets 520 associated with each port bundle. The classification index for the super packet can include port bundle entries 540 for each port bundle. Additionally, the super packet sub factory can extract classification parameters common to all of the port bundles in the super packet, including the source edge, destination edge, sequence number, status bits, index type, versions, and the number of port bundles. After the super packet is constructed, the super packet can be split across the various lambdas link layer processing and transportation to optical switch core 230. While the construction of super packet 500 has been described with reference to the aggregation of port bundles, it should be noted that, in one embodiment of the present invention, data packets can be directly aggregated into a super packet without first being placed in port bundles or can be aggregated into other types of bundles depending on the configuration of router 200. Regardless of the type of bundling employed—if any bundling is employed at all—the classification index can include a bundle entry (e.g., port bundle entry 540) to aid in the disassembly of the super packet.

As discussed, the classification index 510 for super packet 500 can include a classification index common overhead 530, a bundle entry 540 and per packet entries 550 for each of the data packets in a port bundle. Table 1 summarizes the information that can be contained in the packet classification index common overhead 530 for one embodiment of the present invention. Table 1 includes the field name, the number of bits and comments relating to the field. It should be noted that the parameters provided in Table 1 are exemplary only.

Although the present invention has been described in detail herein with reference to the illustrative embodiments, it should be understood that the description is by way of example only and is not to be construed in a limiting sense. It is to be further understood, therefore, that numerous changes in the details of the embodiments of this invention and additional embodiments of this invention will be apparent to, and may be made by, persons of ordinary skill in the art having reference to this description. It is contemplated that all such changes and additional embodiments are within the spirit and true scope of this invention as claimed below.

US 8,116,315 B2

11

TABLE 1

Example Classification Index Overhead		
Field Name	Number of Bits	Comments
Source Edge	4	16 Edges, 0000 ⇔ 1111
Destination Edge	4	16 Edges, 0000 ⇔ 1111
Sequence Number	16	0 ⇔ 65,535
Status Bits	4	Reserved/Empty
Number of Port Bundles	4	0 ⇔ 15

As can be seen from Table 1, one embodiment of the packet classification index common overhead **530** can include a source edge designation to identify the ingress edge unit **210** that is sending the super packet **500** and a destination edge designation to identify the destination egress edge unit **220**. In the case of a router with 16 ingress edge units and 16 egress edge units, this data can be represented with four bits from 0000 through 1111. Common overhead **530** can also include a sequence field for diagnostics, which could include an unsigned integer value that can be incremented every time a super packet is formed in a super packet sub factory destined for a particular egress edge unit. The destination egress edge unit should generally see the sequence number increasing in packets sent from each ingress edge unit. The sequence number field can wrap around from a maximum value, in this example 65,535, and begin again at zero.

The classification index common overhead **530** could also include a status bit to indicate the presence or absence of some option determined by the router administrator or other party or to indicate that there is an alternative processing mechanism for processing the super packet. If there is a reserved flag in this field, it could be an indication that the bits associated with the field are reserved for future use. Or, an empty flag in this field could indicate that there are no packets in the super packet **500** that need to be serviced. Additionally, as indicated by Table 1, super packet common overhead **530** can include a number of port bundles indicating the number of port bundles included in super packet **500**. The number of port bundles can be used by the destination egress edge unit **220** to properly disassemble super packet **500**. However, in some cases there may be no port bundles in super packet **500**, as might occur if the super packet did not contain any data packets, if the super packet contained only one data packet, or the data packets in the super packet were not further categorized into port bundles.

In addition common overhead **530**, classification index **510** can include a port bundle entry **540** for each port bundle in super packet **500**. Port bundle entries **540** can contain classification parameters that are common to each data packet within a port bundle. Table 2 provides exemplary field names, number of bits and comments for each field in one embodiment of port bundle entry **540**.

TABLE 2

Example Port Bundle Classification Parameters		
Field Name	Number of Bits	Comments
Offset to Port Bundle	24	Depends on Super Packet size
Index Type	4	Types are described in Table 2
Version	4	Initial: 0000
Status Bits	4	Reserved/Tail Frag/Head Frag
Number of PPEs	12	Depends on Super Packet size

12

As can be understood from Table 2, port bundle entry **540** can include an indication of the offset to port bundle which provides the starting addresses of the port bundle overhead data, if any, the per-packet entries; e.g., the classification index entries for each individual packet, and the packet data. In port bundle entry **540**, the index type can define the per-port bundle overhead information and the format of the per packet entries. The index types are described in more detail in conjunction with Tables 5-13. The version field of port bundle entry **540** can allow for evolution of the table of contents to support different configurations and modifications to the fields. Based on the combination of the index type and version, router **200** can select the appropriate algorithm to process port bundle entry **540** and per packet entries **550**. As with common overhead **530**, the status bits field of port bundle entry **540** can be used as an indicator of the presence or absence of an option or an indication to use an alternative processing mechanism. If this field indicates that it is reserved, the bits can be reserved for future use. The status field can also include a head or tail flag indicate the presence of a fragmented data packet in a port bundle.

While port bundles have, to this point, been described in terms of containing whole data packets, each port bundle may contain portions of a data packet that has been fragmented. A head fragment of a data packet can be created by super packet processor **270** when a super packet can not contain any additional complete data packets, but space remains free within the super packet. The packet can be split such that the remaining space in the super packet is occupied by the head fragment of a data packet. The super packet sub factory handling the super packet can duplicate the per packet information for the data packet being split and place the tail fragment and duplicated classification information in a buffer. The values for packet length can be adjusted for both the head and tail fragments of the data packet. The super packet subfactory can then check the head fragment bit in port bundle entry **540** for a port bundle that can accommodate the head fragment and place the head fragment at the end of the port bundle. In a later port bundle, the subfactory can check the tail fragment bit in the port bundle entry **540** for the later port bundle and place the tail fragment at the beginning of the later port bundle. Because packets can be fragmented to fill up super packets, the present invention can ensure super packets are filled to capacity before transporting the super packets to their destinations.

In addition to the fields already discussed, port bundle entry **540**, as indicated by Table 2 can include a number of per-packet entries field to indicate how many per-packet entries are present for a particular port bundle. This value can be used by egress edge unit **220** to determine how many per packet entries must be processed for a port bundle. Thus, in one embodiment of the present invention port bundle entry **540** can include an offset to port bundle field, and index type, a version type, a status bit (e.g., reserved, head frag or tail frag) and an indication of the number of per packet entries.

While each of the fields illustrated in Table 2 has been discussed in detail, Table 3 is provided to further explicate the index type field. As illustrated in Table 3, the various index types can be assigned a numeric code (e.g., 0000 for "Best Effort") that can appear in port bundle entry **540** of the classification index **510**. Table 3 includes an exemplary list of index types and the numerical codes that can be used to represent the index types.

US 8,116,315 B2

13

TABLE 3

Yotta Packet Classification Index Type	
Index Type	Codepoint
Best Effort	0000
Quality of Service Queue	0001
Quality of Service Queue with per packet QoS Codepoint	0010
Quality of Service Queue with per packet QoS Weighting	0011
Common QoS Queue Parameter	0100
Common QoS Queue and QoS Weighting Parameters	0101
Common Packet Size and QoS Queue Parameters	0110
Common Packet Size, QoS Queue and QoS Weighting Parameters	0111
Reserved	1000 ↔ 1111

As previously noted, the format of the per packet entry is dependant on the index type. Thus, for example, a per packet entry for a best efforts index can have a different format than a per packet entry for a quality of service queue index.

Turning now to each of the index types, best efforts index can be used when no quality of service processing is desired and can include the egress port for a particular packet. The per-packet entry for a best effort index can include the length of the packet and a multi-cast bit. Generally, if the multi-cast bit is set, there will be multiple per-packet entries for a particular data packet. Thus, there will be fewer packets in super packet **500** than there are per-packet entries in the packet classification index **510**. If the multi-cast bit is set when a particular packet is processed at egress edge unit **220**, egress edge unit **520** will direct the packet to the first port indicated in the first per-packet entry for that packet and then to the port indicated in the second per-packet entry for that packet and so on until all the per packet entries for the data packet are exhausted. This allows a particular data packet to be sent to multiple ports as addressed by the per-packet entries. To terminate multicasting, the multicast bits can be left unset on the last per-packet entry for a particular packet so that egress edge unit **220** can move on to the next packet. Note, however, that if a multi-cast packet is only destined for a single port, it will be processed as normal. Table 4 summarizes exemplary information that can be included in a per-packet entry for a best efforts index.

TABLE 4

Example Best Effort Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ↔ 1111

In addition to a best efforts index, there can also be a quality of service queue index. The per-packet entry for a quality of service queue index can include a multi-cast flag as previously described, the packet's length, the destination port number and the quality of service queue for the data packet to which the per packet entry pertains. Operators of router **200** can configure router **200** to have a large number of quality of service queues to be used in conjunction with a scheduler algorithm to implement packet routing priorities. Table 5 summarizes the information that could be included in one embodiment of a per-packet entry for a quality of service queue index.

14

TABLE 5

Example Quality of Service Queue Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ↔ 1111
Queues	4	16 queues, 0000 ↔ 1111

Again, the per-packet entry could include a multicast bit, the length of the packet, a destination port, as indicated by 0000 through 1111, and a queue, which in the case of 16 queues could be indicated by 0001 through 1111.

In addition to the information provided in a per-packet entry for a quality of service queue index, the per-packet entry for a quality of service queue with code point index could include a quality of service code point. The code point could be defined by the administrator of router **200** and could be used by egress edge unit **220** to select various processing operations. For example, a code point could indicate a drop probability category or a QoS processing option. Table 6 summarizes the information that could be included in one embodiment of a quality of service queue with code point index per-packet entry.

TABLE 6

Example Quality of Service Queue with Codepoint Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ↔ 1111
Queues	4	16 queues, 0000 ↔ 1111
Codepoint	4	16 codepoints, 0000 ↔ 1111

A quality of service queue with waiting index per packet entry could include a quality of service weighting factor. A weighting factor can be defined by the administrator of router **200** and can be consistent with the port configuration of egress edge unit **220**. For example, the super packet processor **270** could implement token bucket weighting, or other weighting schemes as would be understood by those of ordinary skill in the art, on packets received at ingress edge unit **210**. Table 7 indicates the entries that could be used in one embodiment of a per-packet entry for quality of service queue with weighting index.

TABLE 7

Example Quality of Service Queue with Weighting Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ↔ 1111
Queues	4	16 queues, 0000 ↔ 1111
Weighting Factor	8	QoS Parameter

Additionally, the index can include a common quality of service queue. This index type can include an addition to port bundle overhead entry **540** in addition to a per-packet entry data. Port bundle overhead entry **540** can include a queue field for a common quality of service queue index, which can be located at the port bundle offset address, and can indicate a

15

egress edge unit queue number, while the per-packet entry can contain a multi-cast flag, the packet length and the destination port number. Because the quality of service is set in the port bundle information, all the packets for the port bundle will receive a common quality of service. Tables 8 and 9 summarize the information for the common quality of service queue index for the port bundle overhead queue field and the per-packet entry fields.

TABLE 8

Example Port Bundle Entry for Common Quality of Service Queue Index Type		
Field Name	Number of Bits	Comments
Queue	8	256 queues, 00000000 ⇔ 11111111

TABLE 9

Example Common Quality of Service Queue Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ⇔ 1111

Along with providing common quality of service queue indexing, the present invention can provide common quality of service queue and weighting indexing. This index type, again, includes an addition to the port bundle overhead entry 540, which can again be located in the port bundle offset address, in addition to the per-packet entry. Port bundle overhead queue and weighting factor fields can be used to identify a queue and quality of service weighting parameter that are shared by all per-packet entries for a port bundle. Tables 10 and 11 summarize the information that can be included in the port bundle overhead and the per-packet entries.

TABLE 10

Example Port Bundle Overhead Entry for the Common QoS Queue and Weighting Index Type		
Field Name	Number of Bits	Comments
Queue	8	256 queues, 00000000 ⇔ 11111111
Weighting Factor	8	QoS Parameter

TABLE 11

Example Common Quality of Service Queue and Weighting Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Length	16	Packet size in bytes
Port	4	16 ports, 0000 ⇔ 1111

In another embodiment of the present invention, the index types can include a common packet size and quality of service queue. This index type can include a port bundle overhead area in addition to the per packet entry. Again, the port bundle overhead data can be located at the port bundle offset address, with the per packet entries immediately following the port bundle overhead data, as illustrated in FIG. 5A. The port bundle overhead packet size and queue fields can be used to

16

identify a fixed packet size and quality of service queues used for all per packet entries for a port bundle. Per packet entry can contain a multicast flat and a destination port number. Tables 12 and 13 summarize data that can be included in the port bundle overhead and the per packet entries for a common packet size and quality of service queue index.

TABLE 12

Example Port Bundle Overhead Entry for the Common Packet Size and QoS Queue Index Type		
Field Name	Number of Bits	Comments
Packet Size	16	Packet Size in bytes
Queue	8	256 queues, 00000000 ⇔ 11111111

TABLE 13

Example Common Packet Size and Quality of Service Index Per Packet Entry		
Field Name	Number of Bits	Comments
Multicast	1	Part of Multicast collection if set
Port	4	16 ports, 0000 ⇔ 1111

Because the amount of information included with indexing in per packet entries can offset byte alignment for packets, the super packet 500's packet classification index 220 can include an index padding field in order to maintain byte alignment and packet data. Table 14 provides a summary of the information that can be included in an index padding field.

TABLE 14

Example of Per Packet Entry Index Padding		
Field Name	Number of Bits	Comments
Padding	1 ⇔ 7	As required

To summarize, router 200 can receive individual data packets at ingress edge unit 210 via port 215 and forward the packets to classification index module 260 where classification information (e.g., the destination egress edge unit, destination egress port and quality of service parameters) for an individual data packet can be extracted from the packet's header. The classification information for the individual data packet can be subsequently used in a per packet entry for the data packet in the classification index for the super packet in which the individual data packet is bundled. In one embodiment of router 200, data packets destined for the same egress edge unit 220 that arrived at the same ingress interface port 215 can be aggregated into port bundles at super packet processor 270. Classification information common to each of the data packets within a port bundle can be placed in the port bundle entry 530 of the classification index 510. It should be understood, however, that in other embodiments of router 200, data packets may not be organized into port bundles or may be bundled according to some other criteria such as quality of service parameters or destination egress port, and the format of the classification index 510 can be configured to accommodate various bundling schemes. At a super packet sub factory (e.g., super packet sub factory 392) port bundles can be aggregated together to form a super packet and classification information common to each of the port bundles in a super packet can be included in super packet overhead 520 of classification index 510. Once a super packet 500 has been



US 8,116,315 B2

17

constructed, the super packet **500** can be forwarded to optical switch core **230** and then to the destination egress edge unit **220**.

With reference to FIG. 2, at egress edge unit **220**, the incoming super packet **500** can be forwarded to classification index processing module **265** to perform classification index processing (rather than packet classification). Because classification index **510** of super packet **500** contains classification information for the super packet **500**, port bundles in super packet **500**, and the constituent data packets in super packet **500** that was previously defined at the source ingress edge router **210**, classification index processing module **265** need only perform simple table reading of classification index **510** rather than performing reclassification. Classification index processing module **265** can parse common overhead **520** to determine classification parameters that are common to all of the port bundles in super packet **500**. As discussed in conjunction with Table 1, this information can include the source edge unit, destination edge unit, sequence number, status bits and number of port bundles, if any.

Classification index processing module **265** can also parse the port bundle to determine the starting address of each port bundle, the overhead information for the port bundle (e.g., the index type, version and status bits) and the number of per packet entries, if any, for the port bundle. Egress super packet factory **280** can extract the data packets from the port bundles and classification index processing module **265** can read the per packet entries to determine the destination port **225**, quality of service parameters or other routing information for each data packet. The data packets then be forwarded to appropriate port **225**. Additionally, if there are several QoS queues for a particular port, the data packet can be routed to the proper QoS queue. It should also be recalled that if a data packet is to multicast to server egress ports **225** there can be multiple per packet entries for the data packet. Furthermore, the format of the per packet entries for data packets in a particular port bundle can be determined by the index type in the port bundle entry **540** for that port bundle. Based on the classification information in the per packet entries, the individual data packets of super packet **500** can be routed to the appropriate port.

In one embodiment of the present invention, index classification processing module **265** can be distributed over several components of egress edge router **220**. For example classification index module **260** could determine the destination port for each data packet at egress super packet factory **280** and determine the appropriate QoS queue for each data packet at the destination port. Thus, in this embodiment, the processing of super packet classification index **510** could occur in two stages (e.g., the destination port for a data packet would be determined at egress super packet factory **280**, while the QoS queue for the data packet would be determined at the destination port).

As noted above, data packets can generally be routed to the appropriate egress port **225** based on the classification information contained in the per packet entries. However, if a head frag flag is set in the status bit of a port bundle entry **530**, the last packet in a port bundle can be placed in a fragmentation buffer for the destination port of the fragmented package. When a port bundle arrives, typically in the same super packet **500**, with the tail frag flag set in the status bit of the corresponding port bundle entry **530**, the tail fragment can be forwarded to the fragmentation buffer to be joined with the head fragment. The combined data packet can then be forwarded to the port with which the fragmentation queue is associated. FIG. 5D shows diagrammatically how this head frag/tail frag process can be implemented. Initially, previous

18

head frag (or fragment) **610** is stored in frag buffer **620**. As super packet **500** arrives, it can contain a current head frag **630** and a current tail frag **640**. If super packet **500** contains a current tail frag **640**, then previous head frag **610** will always exist in frag buffer **620** (because it came with the previous super packet). The current tail frag **640** is joined with previous head frag **610** (as indicated by arrow **1**) to create a packet. After this newly created packet is moved out of frag buffer **620**, current head frag **630** is moved into frag buffer **620** (at position **00**) and the next arriving super packet **500** will provide its tail fragment (shown as next tail frag **650**).

The present invention provides a system and method for classifying data packets at an ingress edge unit of a router/switch without requiring reclassification of the data packets at the destination egress edge unit. In contrast to prior art systems in which classification information is typically lost after a data packet or super packet leaves an ingress edge unit, the present invention can place classification information for a data packet or super packet in a classification index for the data packet or super packet. The classification index can then be communicated to the destination egress edge unit along with the data packet or super packet. Because the destination egress edge unit receives classification information (e.g., in the classification index) from the ingress edge unit, the egress edge unit need simply read the classification information to determine the destination port, quality of service queue, etc., rather than reclassifying the data packet. Furthermore, the classification index containing the classification information can be formatted as an easily readable table so that the destination edge router need only employ simple table reading hardware and/or software to determine the destination port, quality of service queue, etc. for a data packet. Thus, the present invention can reduce the software/hardware requirements for the destination edge router and minimize duplicative processing of a data packet.

Although the present invention has been described in detail herein with reference to the illustrative embodiments, it should be understood that the description is by way of example only and is not to be construed in a limiting sense. It is to be further understood, therefore, that the numerous changes in the details of the embodiments of this invention and additional embodiments of this invention will be apparent to and may be made by persons of ordinary skill in the art having reference to this description. It is contemplated that all such changes in additional embodiments are within the spirit and true scope of this invention as claimed below.

What is claimed is:

**1.** A method of routing a plurality of data packets through a network, comprising:

at an ingress edge unit: determining a set of classification parameters for each of the plurality of data packets arriving at the ingress edge unit, wherein the set of classification parameters includes destination information and one or more quality of service (QoS) parameters for the respective data packet and wherein the destination information includes a destination egress edge unit; and constructing a classification index including the QoS parameters and information about a plurality of queues associated with the QoS parameters;

transporting the plurality of data packets and the classification index to the destination egress edge unit; and at the destination egress edge unit, routing each of the plurality of data packets to an associated destination egress port within the destination egress edge unit based on the classification parameters determined at the ingress edge unit and without reclassifying any data packet at the destination egress edge unit.

US 8,116,315 B2

19

2. The method of claim 1, wherein constructing the classification index, comprises incorporating the set of classification parameters for each of the plurality of data packets in the classification index.

3. The method of claim 1, wherein the determining a set of classification parameters for each of the plurality of data packets further comprises:

for each of the plurality of data packets, determining the destination egress edge unit out of a plurality of egress edge units and determining the associated destination egress port out of a plurality of egress ports within the determined destination egress edge unit.

4. The method of claim 3, further comprising accessing a look-up table to correlate a destination IP address to the determined destination egress edge unit and the destination egress port for each of the plurality of data packets.

5. The method of claim 1, wherein the plurality of data packets is subdivided into at least one port bundle, and further comprising:

determining a first set of common classification parameters, wherein the first set of common classification parameters are common to each data packet in a port bundle.

6. The method of claim 5, further comprising:

determining a second set of common classification parameters, wherein the second set of common classification parameters are common to each port bundle; and transporting the first set and the second set of common classification parameters to the destination egress edge unit.

7. A method for data packet processing in a telecommunications system, comprising:

at an ingress edge unit of a router, determining a set of classification parameters for a data packet arriving at the ingress edge unit, wherein the classification parameters include destination information and one or more quality of service (QoS) parameters for the data packet, and wherein the destination information includes a destination egress port of the router;

constructing a classification index including the set of classification parameters for a plurality of data packets, and also including information about a plurality of queues associated with the QoS parameters;

forwarding the classification index to at least one destination edge unit of the router, including a destination edge unit associated with the destination egress port associated with the data packet; and

forwarding the data packet to the destination egress port according to the classification parameters determined at the ingress edge unit and without requiring reclassification of the data packet.

8. The method of claim 7, further comprising configuring an optical core of the router to route the data packet from the ingress edge unit to the destination egress port.

9. The method of claim 8, further comprising:

determining a destination egress edge unit associated with the destination egress port for the data packet; and transporting the data packet to the determined destination egress edge unit.

10. The method of claim 9, further comprising accessing a look-up table to correlate a destination IP address to the determined destination egress edge unit and the destination egress port.

11. The method of claim 7, further comprising:

constructing the classification index to include the destination egress edge unit and the destination egress port.

20

12. A system for the classification of data packets in a telecommunications system, comprising:

at least one ingress edge unit coupled to an optical switch core, wherein the at least one ingress edge unit is configured to receive a data packet;

determine classification parameters for the data packet, including one or more quality of service (QoS) parameters;

communicate the data packet and the classification parameters associated with the data packet to the optical switch core, wherein the at least one ingress edge unit is configured to communicate the classification parameters as part of a classification index including the classification parameters for a plurality of data packets and information about each of a plurality of queues associated with the QoS parameters; and

at least one egress edge unit coupled to the optical switch core, wherein the at least one egress edge unit is configured to receive the data packet;

process the classification parameters associated with the data packet; and

route the data packet to a destination egress port within the at least one egress edge unit according to the classification parameters determined at the at least one ingress edge unit and without requiring reclassification of the data packet.

13. The system of claim 12, further comprising:

at least one ingress packet link connecting the at least one ingress edge unit and the optical switch core; and

at least one egress packet link connecting the optical switch core and the at least one egress edge unit,

wherein the classification parameters are communicated to the at least one egress edge unit via the at least one ingress packet link and the at least one egress packet link.

14. The system of claim 12, further comprising:

at least one ingress control link connecting the at least one ingress edge unit and the optical switch core; and

at least one egress control link connecting the optical switch core and the at least one egress edge unit,

wherein the classification parameters are communicated to the at least one egress edge unit via the at least one ingress control link and the at least one egress control link.

15. A method of routing a plurality of data packets through a network, comprising:

at an ingress edge unit, determining a set of classification parameters for each of the plurality of data packets arriving at the ingress edge unit, wherein the set of classification parameters includes destination information and wherein the destination information includes a destination egress edge unit, wherein determining a set of classification parameters for each of the plurality of data packets further comprises, for each of the plurality of data packets, determining a destination egress edge unit out of a plurality of egress edge units and determining a destination egress port out of a plurality of egress ports within the determined destination egress edge unit, and wherein determining a set of classification parameters for each of the plurality of data packets further includes determining a set of quality of service (QoS) parameters associated with each of the plurality of data packets;

21

constructing a classification index including the QoS parameters for each of the plurality of data packets, wherein the constructing comprises including, in the classification index, information about each of a plurality of queues associated with the QoS parameters; 5  
transporting the plurality of data packets to the destination egress edge unit;  
at the destination egress edge unit, routing each of the plurality of data packets to the associated destination egress port within the destination egress edge unit based on the classification parameters determined at the ingress edge unit and without reclassifying any data packet at the destination egress edge unit; and  
forwarding the classification index to the destination egress 15 edge unit.

16. A method of routing a plurality of data packets through a network, comprising:

at an ingress edge unit, determining a set of classification parameters for each of the plurality of data packets arriving at the ingress edge unit, wherein the set of classification parameters includes destination information and wherein the destination information includes a destination egress edge unit, wherein determining a set of classification parameters for each of the plurality of data 25 packets further comprises, for each of the plurality of data packets, determining a destination egress edge unit out of a plurality of egress edge units and determining a destination egress port out of a plurality of egress ports within the determined destination egress edge unit, and wherein determining a set of classification parameters for each of the plurality of data packets further includes determining a set of quality of service (QoS) parameters associated with each of the plurality of data packets; 35

constructing a classification index including the QoS parameters for each of the plurality of data packets, wherein the constructing comprises constructing a QoS vector, the QoS vector being code points of compressed QoS parameters, and placing the QoS vector in the classification index; 40

transporting the plurality of data packets to the destination egress edge unit;

at the destination egress edge unit, routing each of the plurality of data packets to the associated destination egress port within the destination egress edge unit based on the classification parameters determined at the ingress edge unit and without reclassifying any data packet at the destination egress edge unit; and  
forwarding the classification index to the destination egress 50 edge unit.

22

17. A method of routing a plurality of data packets through a network, comprising:

at an ingress edge unit, determining a set of classification parameters for each of the plurality of data packets arriving at the ingress edge unit wherein the set of classification parameters includes destination information and wherein the destination information includes a destination egress edge unit; and further comprising at the ingress edge unit:

creating a port bundle comprising data packets including a first set of common classification parameters;

extracting common information from the data packets in the port bundle;

storing the common information and classification information for each of the plurality of data packets in an overhead for the port bundle; and

assembling a plurality of port bundles including a second set of common classification parameters into a super packet;

transporting the plurality of data packets to the destination egress edge unit; and

at the destination egress edge unit, routing each of the plurality of data packets to an associated destination egress port within the destination egress edge unit based on the classification parameters determined at the ingress edge unit and without reclassifying any data packet at the destination egress edge unit.

18. The method of claim 17, further comprising at the ingress edge unit:

extracting common information from the plurality of port bundles; and

storing the common information and classification information for each of the plurality of port bundles in an overhead for the super packet.

19. The method of claim 18, further comprising at the ingress edge unit:

constructing a classification index for the super packet, the classification index including classification parameters for each of the plurality of data packets in the super packet; and

storing the classification index in an overhead of the super packet.

20. The method of claim 17, wherein a fragment of a fragmented data packet is stored one of the plurality of port bundles in the super packet to fill a remaining space of the super packet and an associated flag is set to indicate which portion of the fragmented data packet is stored in the super packet.

21. The method of claim 19, wherein the classification index comprises an entry for each of the plurality of data packets in the super packet.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 8,116,315 B2  
APPLICATION NO. : 11/471149  
DATED : February 14, 2012  
INVENTOR(S) : Posey, Jr.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page, item (57), under “Abstract”, in Column 2, Line 8, delete “according the” and insert -- according to the --.

Title Page 2, item (56), under “Other Publications”, in Column 2, Line 1, delete “Integratio”, and insert -- integration”, --.

Title Page 2, item (56), under “Other Publications”, in Column 2, Line 11, delete “1194-Jun.” and insert -- 1994-Jun. --.

Title Page 2, item (56), under “Other Publications”, in Column 2, Line 22, delete “Tuneable” and insert -- Tunable --.

Column 1, line 8, delete “10,138,760,” and insert -- 10/138,760, --.

Column 19, line 2, in Claim 2, delete “index, comprises” and insert -- index comprises --.

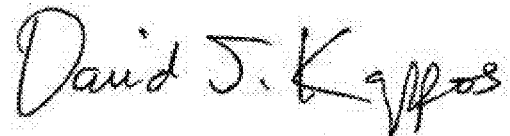
Column 20, line 9, in Claim 12, delete “parameters;” and insert -- parameters; and --.

Column 20, line 26, in Claim 12, delete “according the” and insert -- according to the --.

Column 22, line 4, in Claim 17, delete “data rackets” and insert -- data packets --.

Column 22, line 5, in Claim 17, delete “unit wherein” and insert -- unit, wherein --.

Signed and Sealed this  
Twenty-eighth Day of August, 2012

A handwritten signature in black ink that reads "David J. Kappos". The signature is written in a cursive, flowing style with a large initial "D" and a stylized "K".

David J. Kappos  
*Director of the United States Patent and Trademark Office*

# Exhibit N

---

(10) **Patent No.:** US 7,209,950 B2  
(45) **Date of Patent:** Apr. 24, 2007

(54) **METHOD AND APPARATUS FOR A NETWORK INDEPENDENT SHORT MESSAGE DELIVERY SYSTEM**

(75) Inventors: **Simon Bennett**, Santiago (CL); **Luis Samra**, Miami, FL (US); **Gustavo Jimenez**, Plantation, FL (US)

(73) Assignee: **ZonaMovil.com, Inc.**, Miami, FL (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 515 days.

(21) Appl. No.: **09/921,167**

(22) Filed: **Aug. 2, 2001**

5,903,726	A *	5/1999	Donovan et al. ....	709/206
6,018,657	A *	1/2000	Kennedy et al. ....	455/426.1
6,094,578	A *	7/2000	Purcell et al. ....	455/426.1
6,094,587	A *	7/2000	Armanto et al. ....	455/567
6,097,960	A *	8/2000	Rathnasabapathy et al. ....	455/461
6,263,212	B1 *	7/2001	Ross et al. ....	455/466
6,363,431	B1 *	3/2002	Hammer et al. ....	709/249
6,462,646	B2 *	10/2002	Helferich ....	340/7.21
6,535,746	B1 *	3/2003	Yü et al. ....	455/466
6,549,937	B1 *	4/2003	Auerbach et al. ....	709/206
6,660,456	B1 *	5/2003	Lohtia et al. ....	455/445
6,603,974	B1 *	8/2003	Rollender ....	455/466
6,735,439	B2 *	5/2004	Bowman et al. ....	455/427
2001/0016495	A1 *	8/2001	Chandnani et al. ....	455/445
2002/0032800	A1 *	3/2002	Phuskarı et al. ....	709/246
2004/0171396	A1 *	9/2004	Carey et al. ....	455/466

## FOREIGN PATENT DOCUMENTS

(65) **Prior Publication Data**  
US 2002/0112014 A1 Aug. 15, 2002

EP	0 777394 A1	6/1997
EP	777394 A1 *	6/1997

(Continued)

### Related U.S. Application Data

(60) Provisional application No. 60/225,603, filed on Aug. 15, 2000.

*Primary Examiner*—Nathan J. Flynn

*Assistant Examiner*—Ashok Patel

(74) *Attorney, Agent, or Firm*—Norman E. Henderson

(51) **Int. Cl.**  
*G06F 15/16* (2006.01)  
*H04L 29/08* (2006.01)

(52) **U.S. Cl.** ..... 709/206; 709/238; 709/230;  
455/414.4

(58) **Field of Classification Search** ..... 455/414.1,  
455/414.2, 414.3, 414.4, 456.3, 414, 428,  
455/517, 518, 522, 560; 709/206, 246; 370/351-355,  
370/466-469, 401  
See application file for complete search history.

(57) **ABSTRACT**

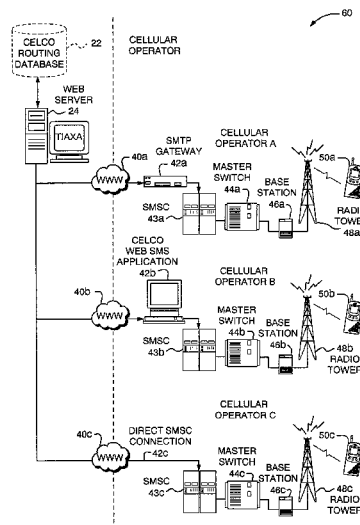
Techniques are described for facilitating communication among a plurality of different telecommunications systems. Communications from a sending network are forwarded to a server that places the communications in a format acceptable to a second receiving network. The server maps an incoming message into any one or more of a variety of formats in accordance with a format acceptable by a receiving network. These communications may include, for example, short messages service (SMS) messages in which the sending and receiving telecommunications systems each have different routing information, such as different electronic addressing formats.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,621,727 A 4/1997 Vaudreuil  
5,852,660 A \* 12/1998 Lindquist et al. .... 379/230

### 38 Claims, 18 Drawing Sheets



**US 7,209,950 B2**

Page 2

---

	FOREIGN PATENT DOCUMENTS	WO	WO 99/11078	3/1999	
EP	0 959600 A1	11/1999	WO	WO 99/33226	7/1999
EP	959600 A1 *	11/1999	WO	WO 9933226 A1 *	7/1999
WO	WO 97/20442	6/1997	WO	WO 00/41533	7/2000
WO	WO 97/36434	10/1997			
WO	WO 9810608 A3 *	3/1998			

\* cited by examiner



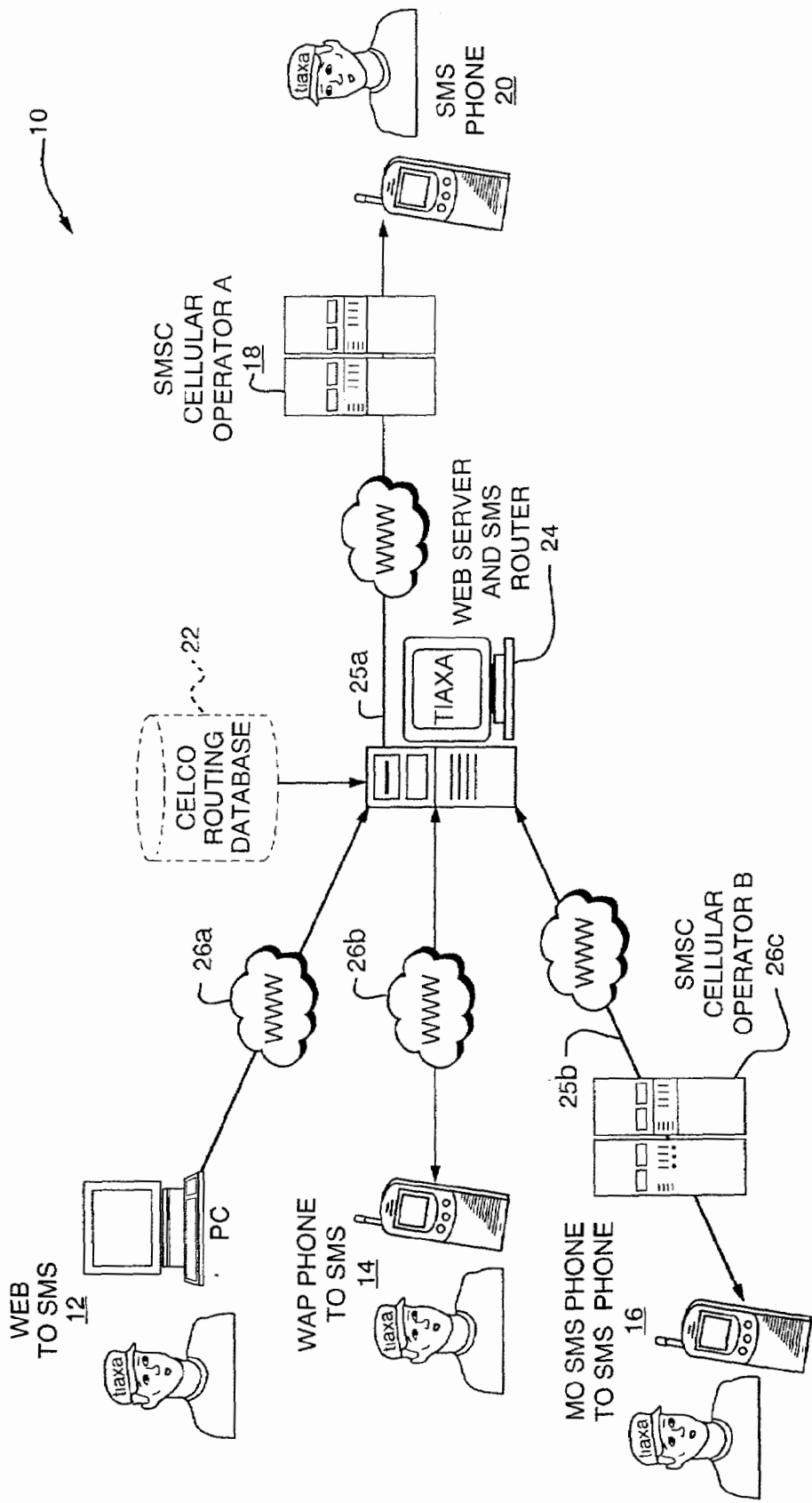


FIG. 1

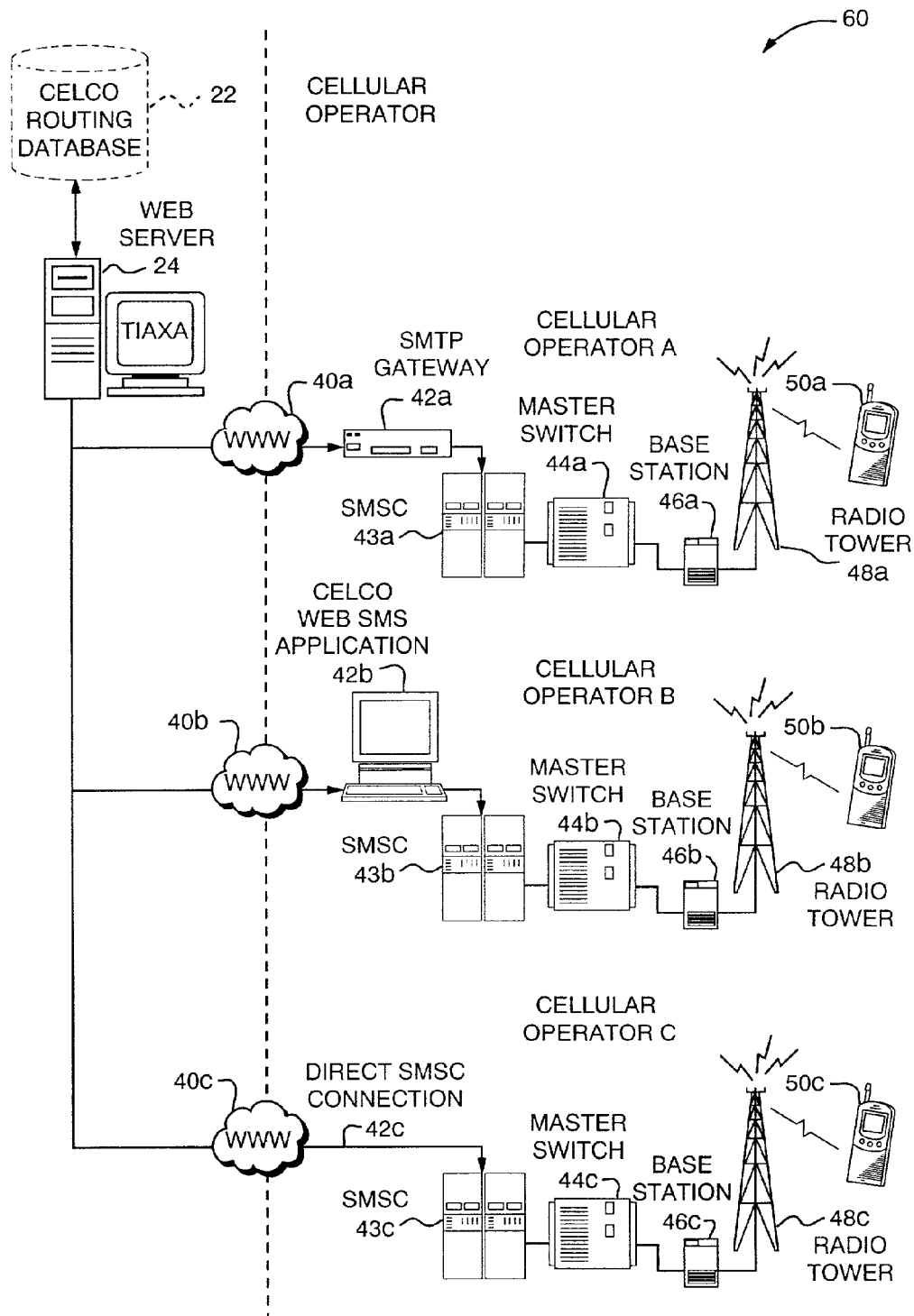
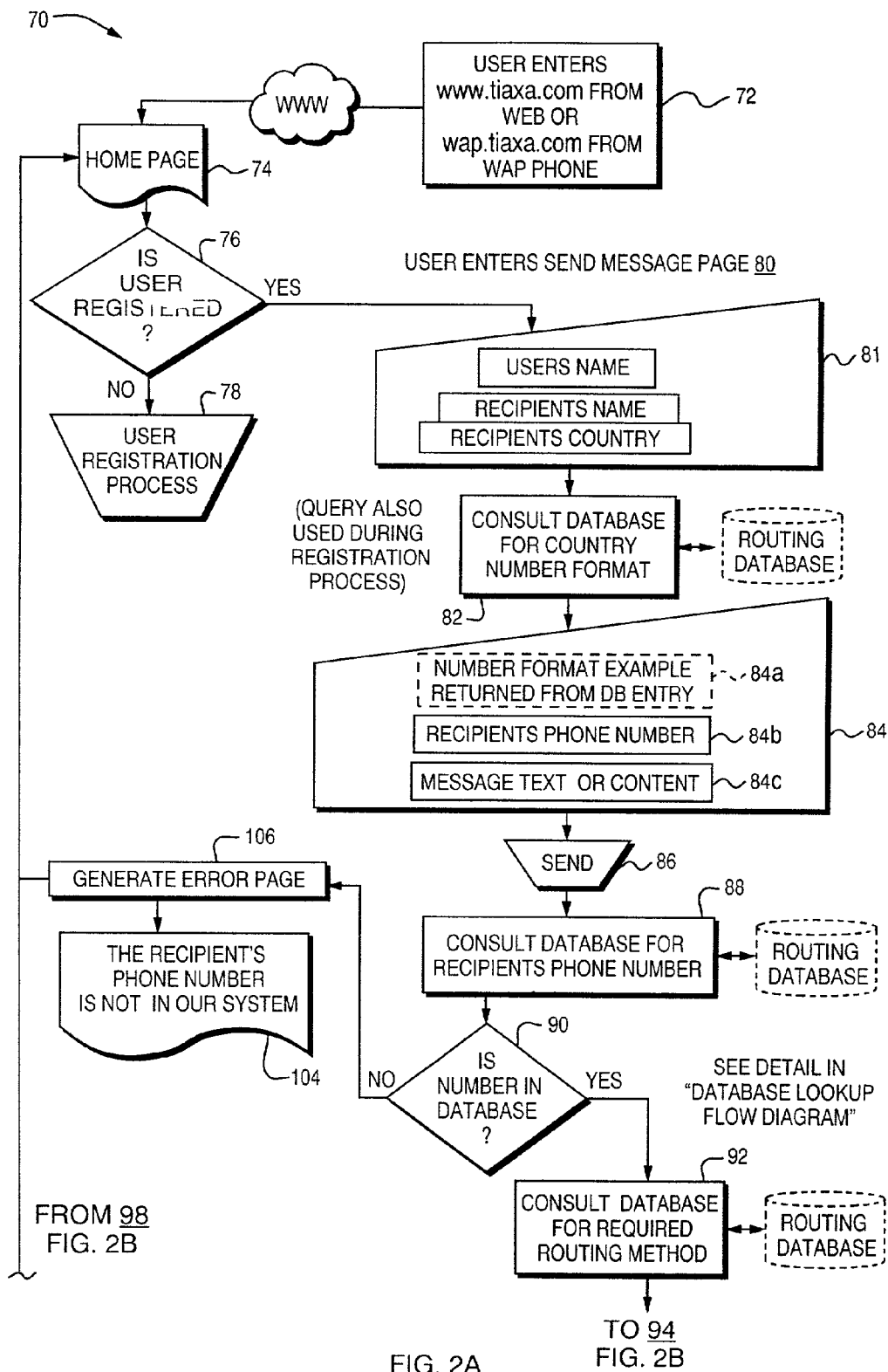


FIG. 1A



U.S. Patent

Apr. 24, 2007

Sheet 4 of 18

US 7,209,950 B2

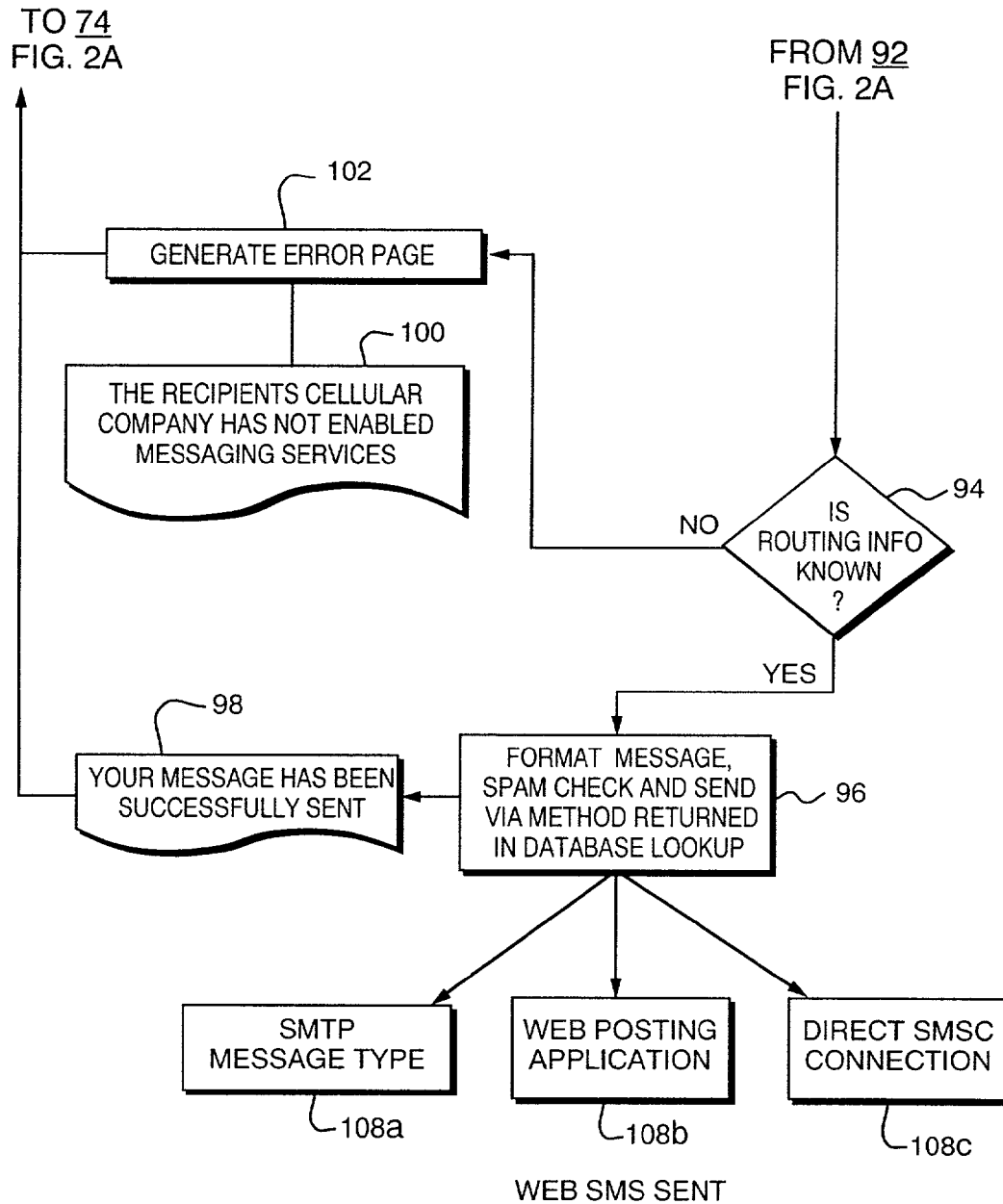


FIG. 2B

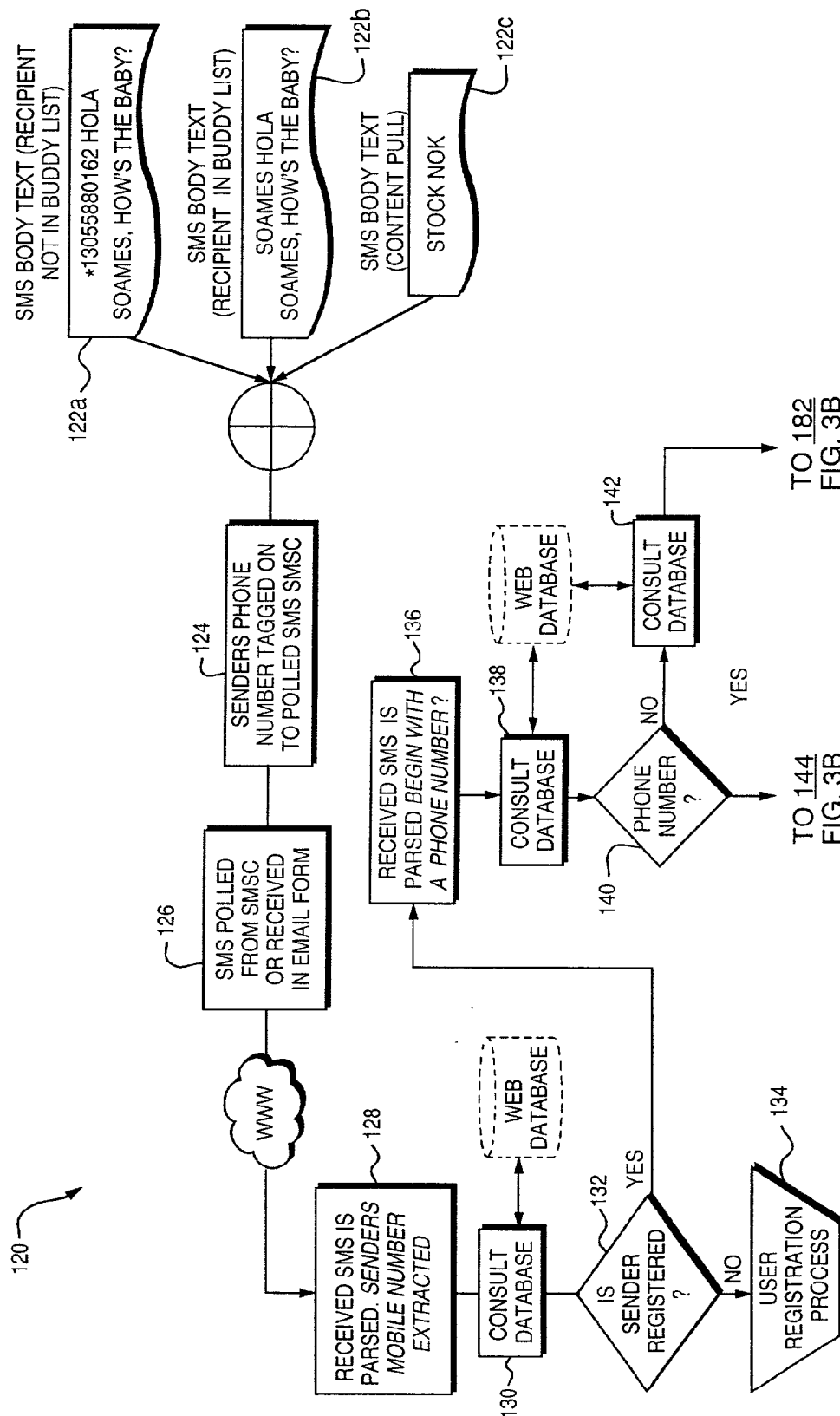
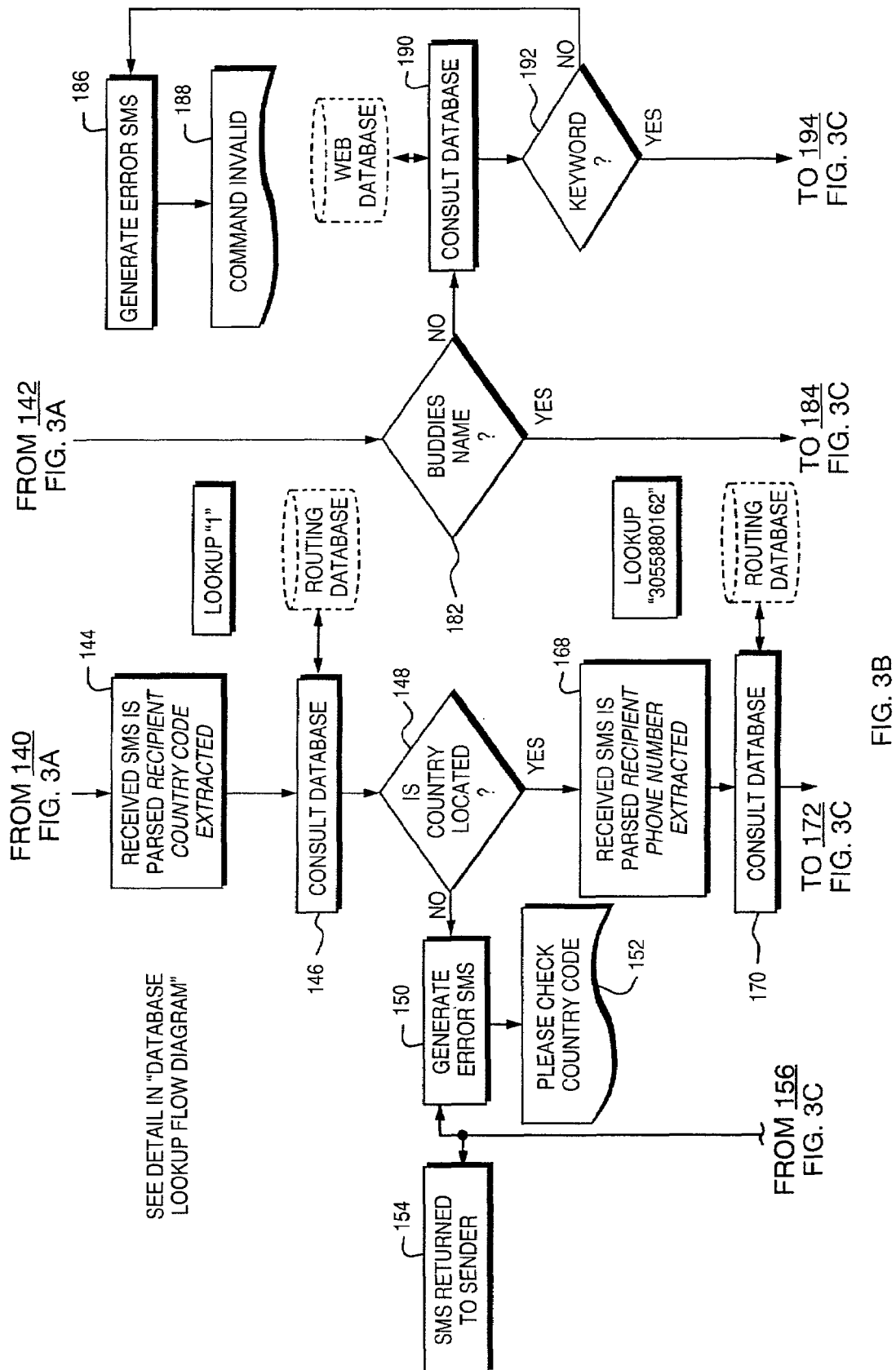
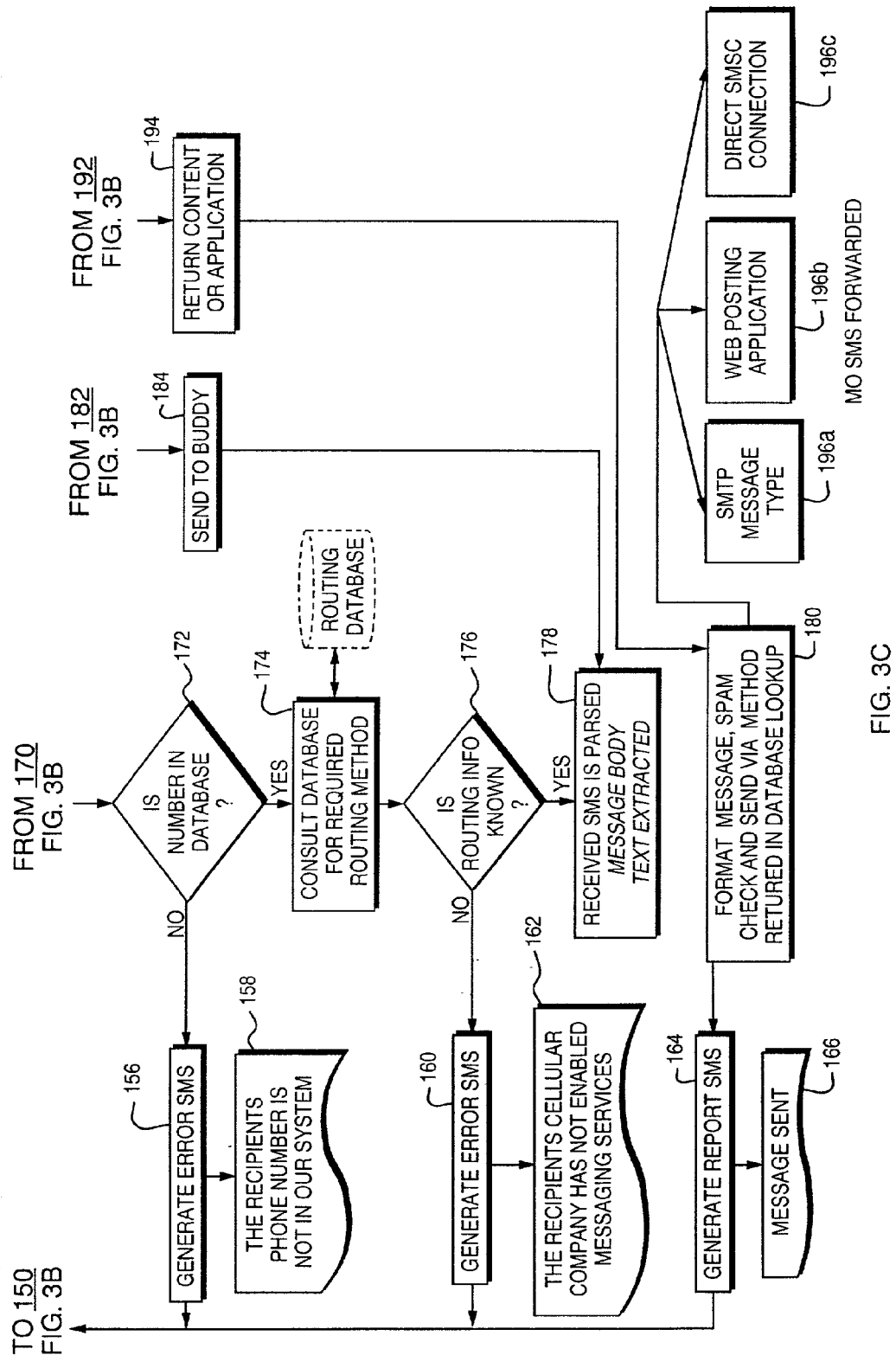
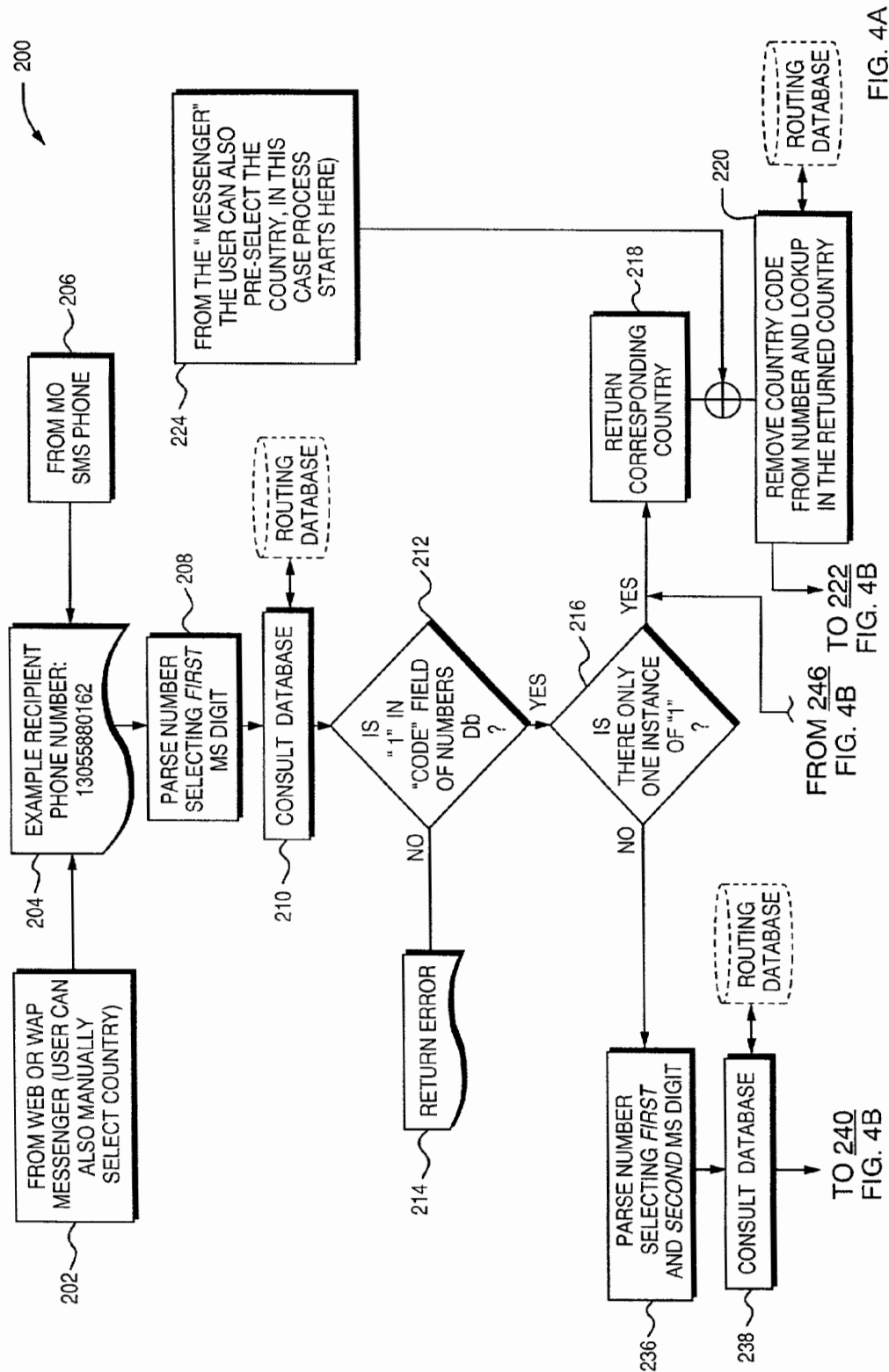


FIG. 3A









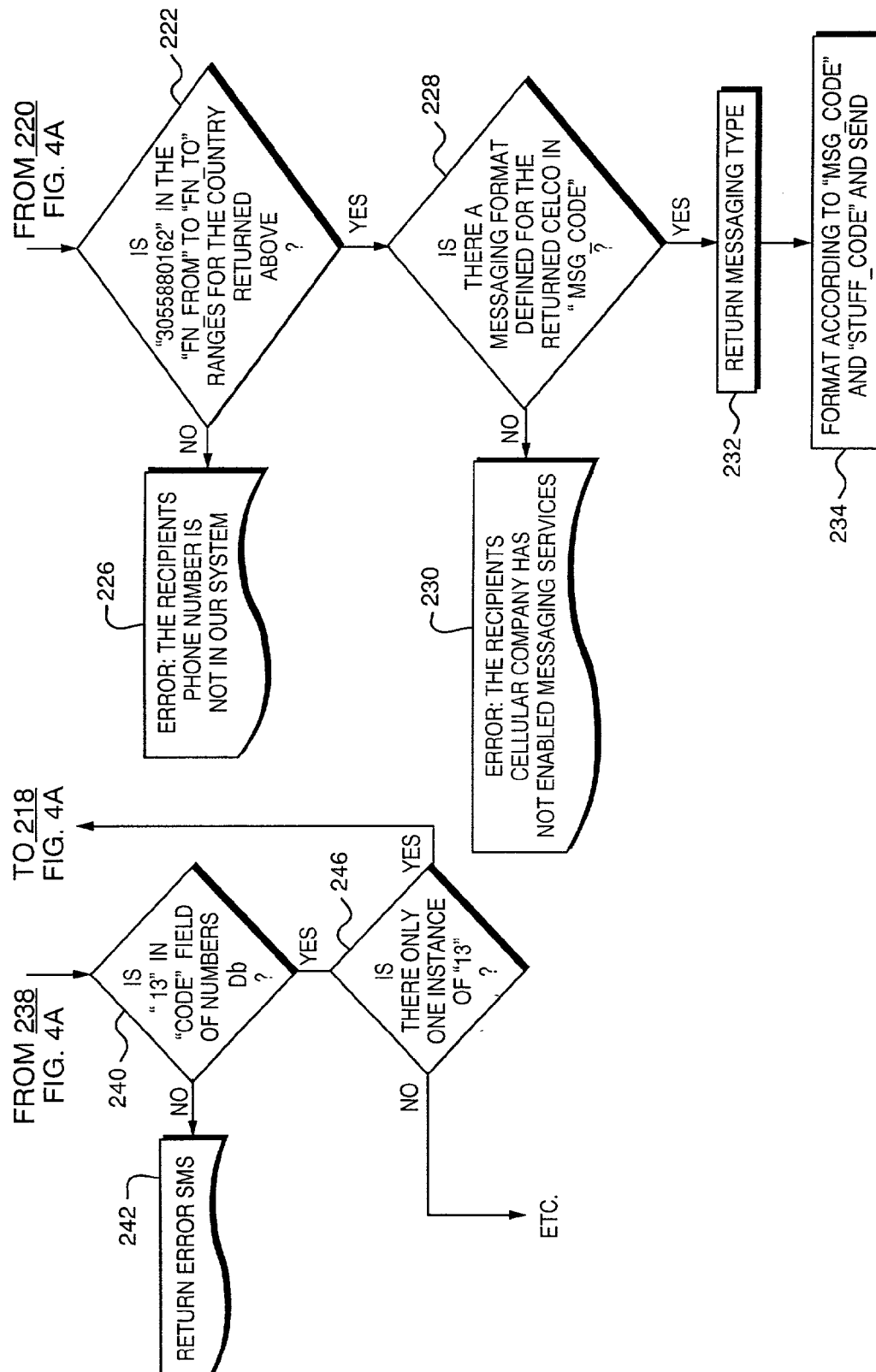


FIG. 4B

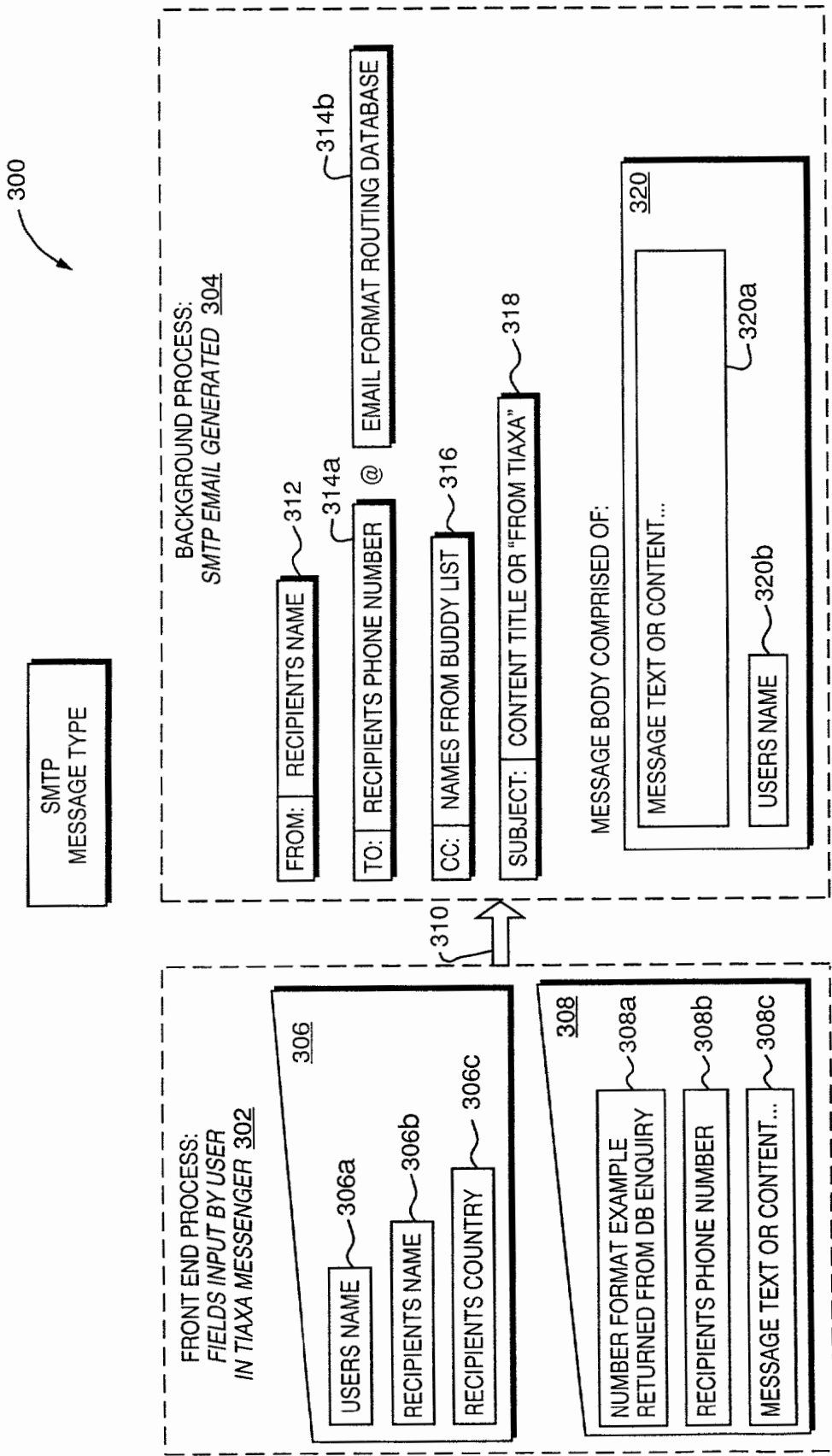


FIG. 5

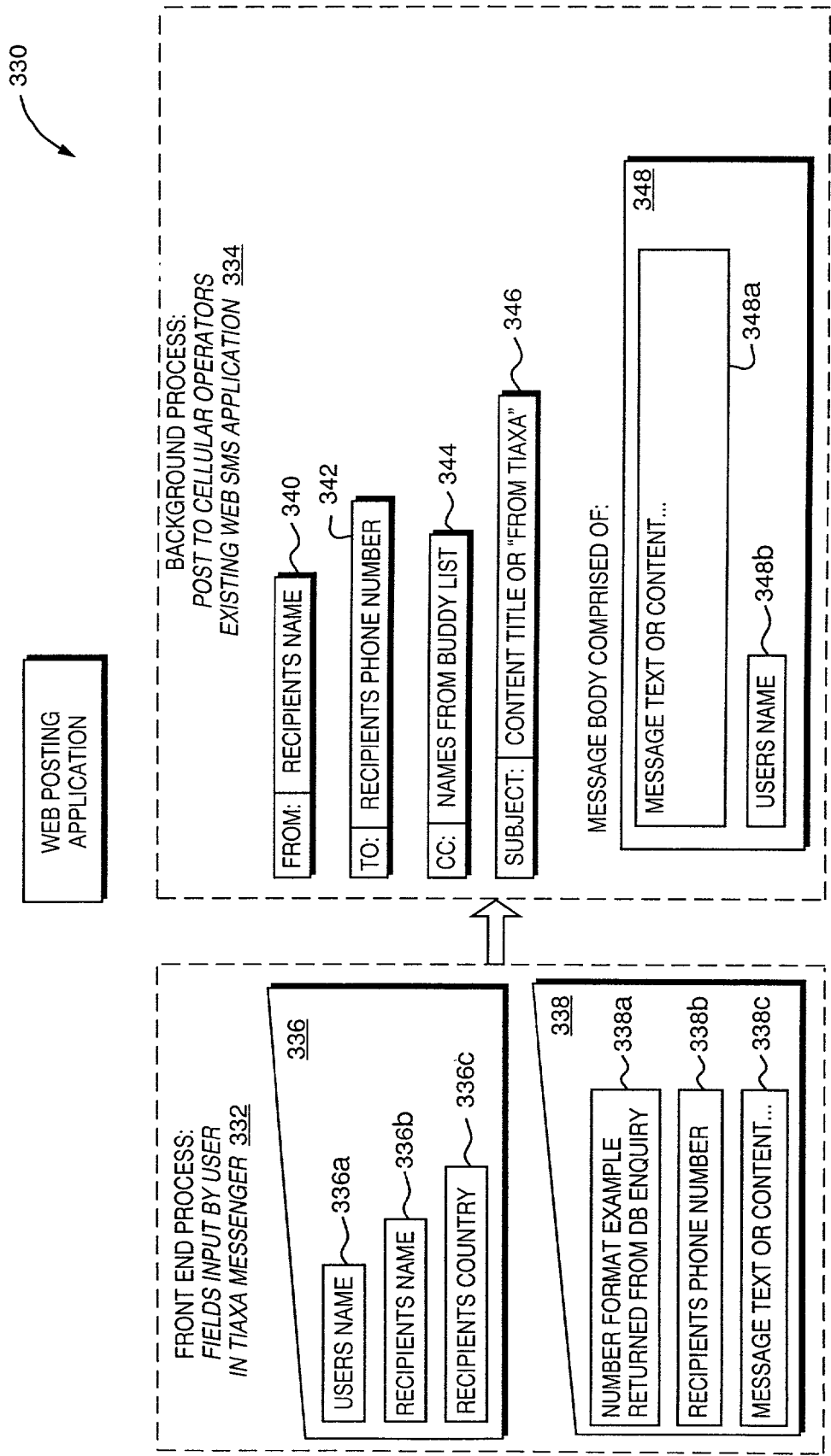


FIG. 6

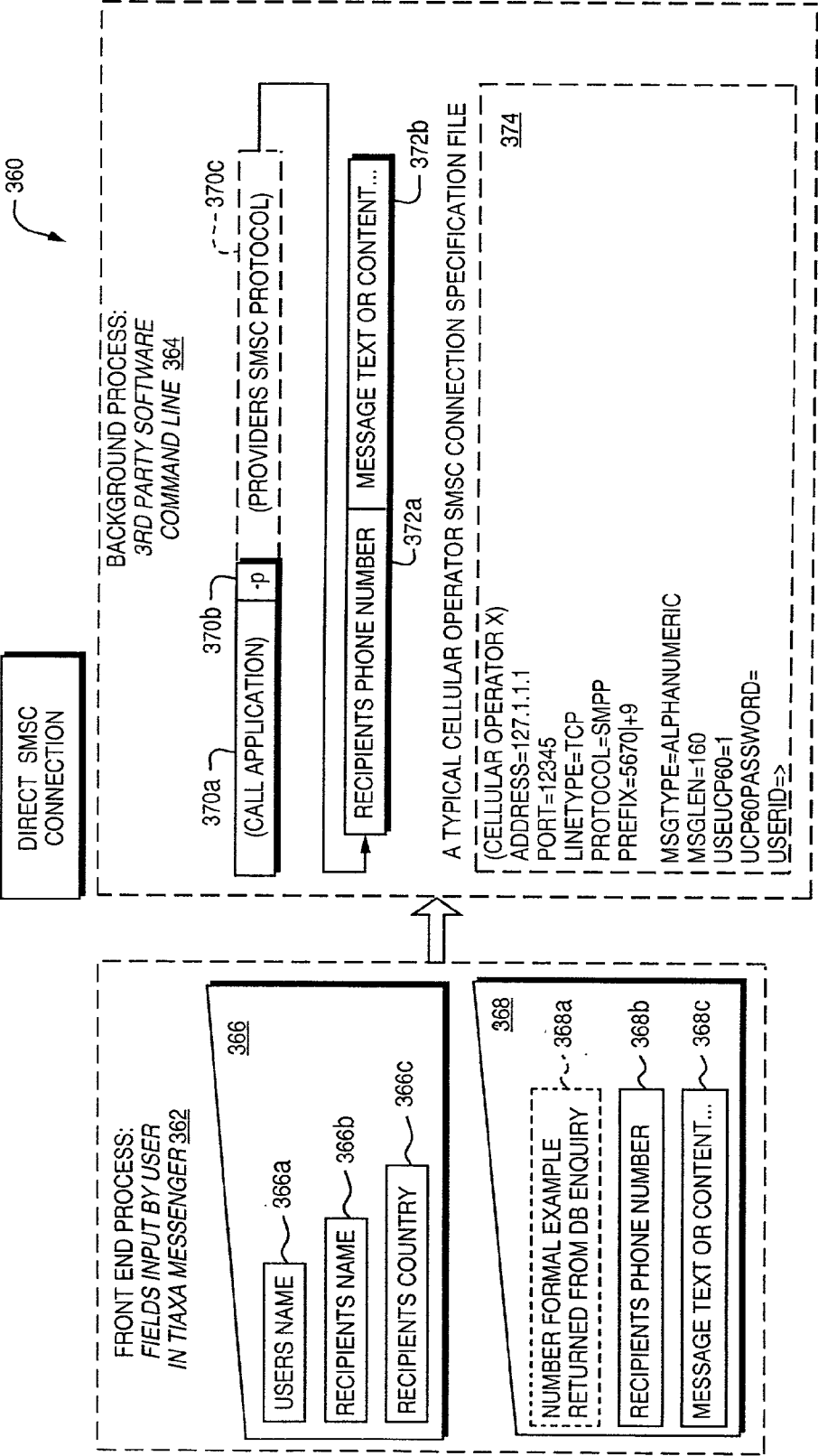


FIG. 7

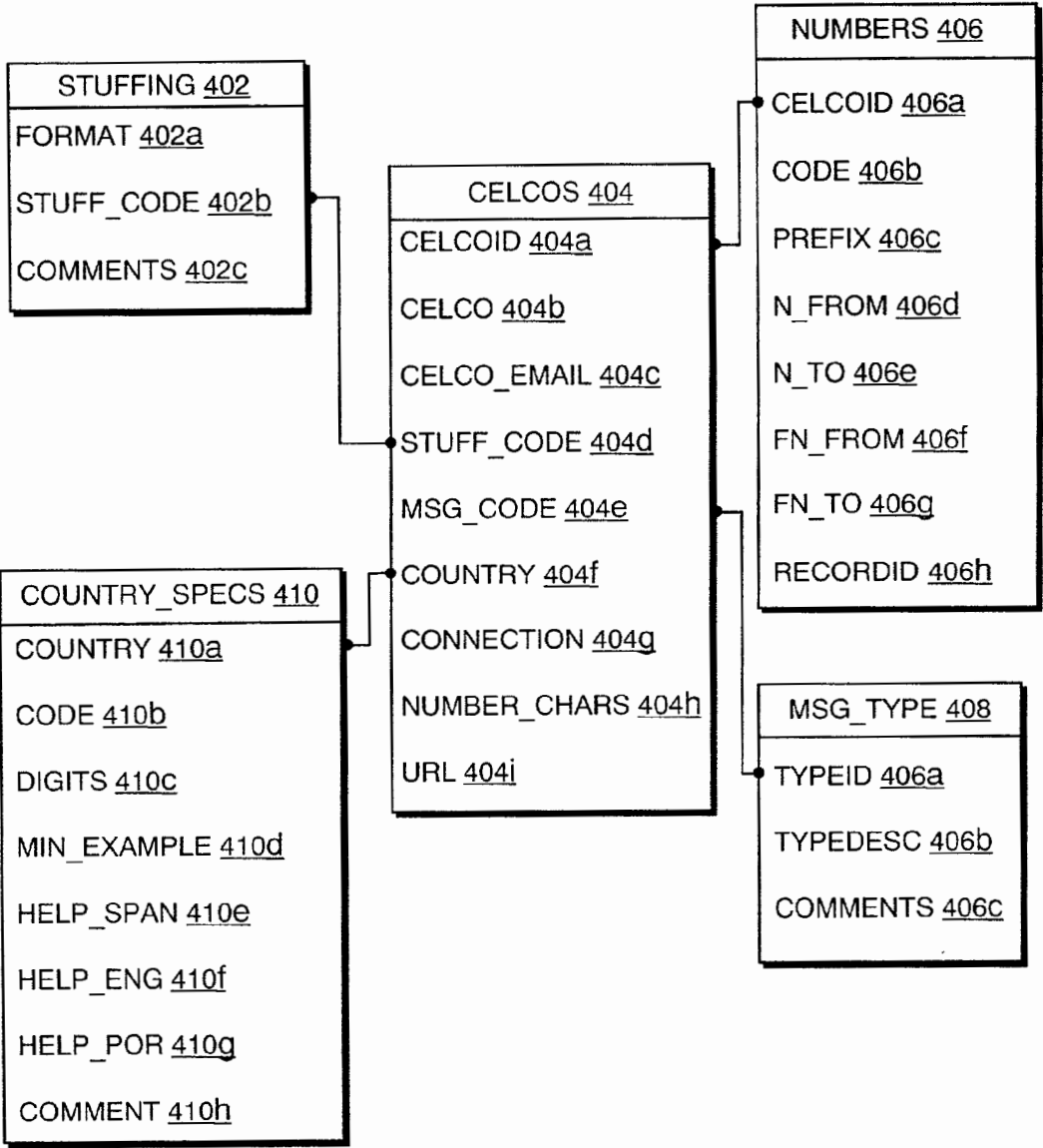


FIG. 8



EXAMPLE OF CONTENTS OF "STUFFING" TABLE 402

FORMAT 402a	STUFF_CODE 402b	COMMENTS 402c
NO COMMENTS	0	
(number)@email	1	
(prefix)(number)@email	2	
(stuffed"0")(prefix"15")(number)@email	3	
(stuffed"1")(area)(number)@email	4	
(stuffed"15")(number)@email	5	
(stuffed"52")(prefix)(number)@email	6	
(stuffed"0")(prefix)(number)@email	7	
"mensajes"@email	8	CELCO X...ALL EMAILS ARE SENT TO mensajes@email
"nexmail"@email	9	CELCO Y...ALL EMAILS ARE SENT TO nexmail@email
(stuffed "706")(number)@email	10	CELCO W
(stuffed "076")(number)@email	11	CELCO W
(NUMBER)	12	http://web.wepostapp.com/
(NUMBER)	13	application

FIG. 9

EXAMPLE OF CONTENTS OF "CELCOS" TABLE 404

CELCOID 404a	CELCO 404b	CELCO_EMAIL 404c	STUFF_CODE 404d	MSG_CODE 404e	COUNTRY 404f	CONNECTION 404g	NUMBER- CHARS 404h	URL 404i
CTIARGE	CTI argentina	cti.comar	2	0	AR	email	100	www.cti.com
BAHACELL	Baja celular	bajacelular.commx	6	0	MX	email	100	www.baja.com
IUSCELL	Iusacell	iusacell.commx	2	0	MX	email	100	www.iusa.com
NORCEL	Norcel	norcel.commx	6	0	MX	email	100	www.norcel.com
PORTACEL	Portatel	unknown	0	0	MX		100	www.porta.com
TELCELMX	Telcel Mexico	unknown	0	0	MX		120	www.telcel.com
BELLPE	BellSouth Peru	unknown	0	0	PE		115	www.bspe.com
NEXTELPERU	Nextel Peru	nextel.compe	9	3	PE	email	115	www.nxtl.com
TELEFOPE	Telefonia Peru	telefon.compe	8	4	PE	email	130	www.telepe.com
6462	360 COMMUNICATIONS- VIRGINIA	atel.com	2	0	US	email	120	www.atel.com
6228	AB CELLULAR HOLDING	mobile.att.net	2	0	US	SMPP	120	www.att.com

FIG. 10

U.S. Patent

Apr. 24, 2007

Sheet 16 of 18

US 7,209,950 B2

EXAMPLE OF CONTENTS OF "NUMBERS" TABLE 406

CELCOID 406a	CODE 406b	PREFIX 406c	N_FROM 406d	N_TO 406e	FN_FROM 406f	FN_TO 406g	RECORDID 406h
TELEFOPE	51	1	8600000	8699999	18600000	18699999	1
TELEFPPE	51	1	9600000	9999999	19900000	19999999	9
BELLEPE	51	1	9500000	9599999	19500000	19599999	15
NEXTELPERU	51	1	8100000	8199999	18100000	18199999	16
BAHACELL	52	1	1010000	1016999	11010000	11016999	17
BAHACELL	52	6	6910000	6919999	66910000	66919999	99
BAHACELL	52	113	95000	96999	11395000	11396999	103
IUSACELL	52	4	7280000	7181999	47280000	47281999	462
IUSACELL	52	4	7282000	7282999	47282000	47282999	463
NORCEL	52	17	450000	459999	17450000	17459999	1029
NORCEL	52	17	460000	469999	17460000	17469999	1030
NORCEL	52	17	580000	589999	17580000	17589999	1031
NORCEL	52	169	10000	19999	16910000	16919999	1032
PORTATEL	52	93	906000	909999	93906000	93909999	1190
PORTATEL	52	93	930000	935999	93930000	93935999	1191
TELCELMX	52		59840000	59849999	59840000	59849999	3805
TELCELMX	52		59910000	59919999	59910000	59919999	3906
TELCELMX	52		59950000	59959999	59950000	59959999	3807
TELCELMX	52		59970000	59979999	59970000	59979999	3808
CTIARGE	54	11	41500000	41509999	1141500000	1141509999	3809
6462	1	804	9890000	9899999	8049890000	8049899999	8120
6462	1	804	9960000	9969999	8049960000	8049969999	8121
6228	1	310	2000000	2009999	3102000000	3102009999	8122

FIG. 11

EXAMPLE OF CONTENTS OF "MESSAGE TYPE" TABLE 408

TYPEID <u>408a</u>	TYPEDESC <u>408b</u>	COMMENTS <u>408c</u>	APPLICATION DESTINATION <u>408d</u>
0	Put [Message] In The Email Body	normal	
1	Put [Message] In The Email Subject		
2	Put [subject] [Message] In The Email Subject		
3	Put [Stuffed Number [Message]] in Email Subject	celco A	
4	Put [Stuffed number] in Email Subject, [Message] in The Email Body	celco Z	
5	Call Web posting:	Celco B	<a href="http://web.wepostapp.com/">http://web.wepostapp.com/</a>
6	Call direct SMSC connection application:	Celco C	application

FIG. 12

EXAMPLE OF CONTENTS OF "COUNTRY SPECS." TABLE 410

COUNTRY 410a	CODE 410b	DIGITS 410c	MIN_EXAMPLE 410d	HELP_SPAN 410e	HELP_ENG 410f	HELP_PORT 410g	COMMENTS 410h
AR	54	10	11(SIN " 15 " ) 412356	HELP TEXT IN SPANISH	HELP TEXT IN ENGLISH	HELP TEXT IN PORTUGUESE	NOTES
BR	55	10	2712345				
EEUU	1	10	305123456				

FIG. 13

US 7,209,950 B2

1

# **METHOD AND APPARATUS FOR A NETWORK INDEPENDENT SHORT MESSAGE DELIVERY SYSTEM**

## **CROSS REFERENCES TO RELATED APPLICATIONS**

This application claims priority from U.S. provisional patent application No. 60/225,603 filed on Aug. 15, 2000.

## **BACKGROUND**

This application generally relates to telecommunications, and more particularly to unification of different messaging systems as may be used in a telecommunication system.

Messaging systems, such as those used in cellular networks for mobile telecommunications, may each employ their own messaging and address formats. This may pose a problem when a message is routed between two different cellular networks. An example of this may occur, for example, when a user from one cellular network or carrier sends a message to another user on a different cellular network.

One particular type of messaging format and service is called the Short Message Service (SMS). In particular with SMS, each SMS message is routed through the mobile network operator network of the receiver of a message. When a sender and receiver are not within the same cellular network, problems may occur in sending messages such as those in accordance with differing SMS formats addressing and protocols used in different networks in connection with the SMS message. The Short Message Service Centers (SMSC) within each particular network such as those used in connection with SMS messages may not comply to any single standard. Compatibility may only be guaranteed within a single digital mobile network. For example, a Global System for Mobile communications (GSM) type of network is a primary system for the SMS implementation network used in Europe. Other regions, such as North and South America, may use different mixed technologies in cellular networks, for example, such as Advanced Mobile Phone Service AMPS Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) as well as GSM. SMSC manufacturers may also each implement different protocols further compounding the mixed varying technologies. Thus, communications between a sender and receiver in which the sender and receiver each use different digital mobile networks, and thus possibly different technologies and standards, may have problems in sending messages between networks.

Thus, it may be desirable and advantageous to have an efficient and improved technique which provides for the unification of different SMSCs, and associated message formats that may be used in different telecommunication systems. It may be desirable and advantageous to provide for improved efficient and more streamlined message sending from a user to a receiver in which the user and the receiver may be in different networks that may not be in accordance with the same messaging standards.

## **SUMMARY OF THE INVENTION**

In accordance with one aspect of the invention is a method executed in a computer system for routing a message from a sender in a first digital mobile network to a receiver in a second different digital mobile network. The message may also be sent from a web page, in either case, a message is

2

forwarded from a sender to a server. The server is connected to the first and second digital mobile network. A routing database is used to relate an identification number associated with the receiver to corresponding routing path information associated with the second digital mobile network. The message is forwarded to the receiver in accordance with the corresponding routing path information.

In accordance with another aspect of the invention is a computer program product for routing a message from a sender in a first digital mobile network to a receiver in a second different digital mobile network. The message may also be sent from a web page, in either case, a message is forwarded from a sender to a server. The server is connected to the first and second digital mobile networks. A routing database is used to relate an identification number associated with the receiver to corresponding routing path information associated with the second digital mobile network. The message is forwarded to the receiver in accordance with the corresponding routing path information.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

Features and advantages of the present invention will become more apparent from the following detailed description of exemplary embodiments thereof taken in conjunction with the accompanying drawings in which:

FIG. 1 is an example of an embodiment of a multi mobile network operator network short message delivery system in a hub formation;

FIG. 1A is a more detailed example of a portion of the network of FIG. 1;

FIG. 2 is an example of an embodiment of a flowchart of steps of one embodiment of processing when a user connects from the internet sending a message to a user on an SMS communication device;

FIG. 3 is an example of an embodiment of a flowchart of steps of one embodiment when an MO SMS (Mobile originating SMS) user sends a message to a receiver using an SMS device the receiver possibly residing on a different network;

FIG. 4 is a flowchart of steps of one embodiment of how to determine routing information;

FIG. 5 is a representation of a mapping that may be performed in sending an SMS message using SMTP e-mail;

FIG. 6 is a representation of an example of sending an SMS message using existing web SMS applications and the mapping performed;

FIG. 7 is a representation of an example of sending an SMS message via direct data connection to an SMSC which an SMSC is a mobile network operator for example;

FIG. 8 is an example of a representation of one embodiment of a data organization of a central routing database; and

FIGS. 9–13 are more detailed examples of tables included in the representation of data in FIG. 8.

## **DETAILED DESCRIPTION OF EMBODIMENT**

Referring now to FIG. 1, shown is an example of an embodiment of a multi-mobile network operator network short message delivery system. It should be noted that although the description included herein relates to SMS as may be routed through mobile network operator networks, the general principles and teachings described in the paragraphs that follow may be generally extended to other types of digital mobile networks employing one or more of a variety of communication devices, and other types of messaging services.



US 7,209,950 B2

3

Included in the multi-mobile network operator network short message delivery system **10** or SMS system **10** is a hub-like network structure that includes a plurality of different types of connections to a server **24**. Generally, the structure shown in the system **10** is a hub-like structure having spokes, such as **12**, **14**, **16** and **20**, representing bi-directional communication paths with the hub in which the server **24** is used to route communications between different message senders and receivers within the system **10**.

The system **10** of FIG. **1** shows different users **12**, **14**, and **16** sending an SMS message to an end user **20** through a server **24** using a routing database **22**.

It should be noted that the routing database **22** may include information in addition to routing information as may be described herein. For example, the routing database may also include additional information on registered users of the server **24**, recipients of messages, and other data that may be described in connection with other flowcharts and descriptions herein.

The user **12** sends an SMS message using the "web" or internet, for example, such as a user connected on a personal computer (PC) through the World Wide Web (WWW) **26a**. This message is forwarded from sending user **12** through the server **24** to the SMS mobile network operator **18** to the end user **20**. Similarly, a sender **14** of a message may use a WAP (wireless application protocol) phone using the WWW **26b** to connect and send a message through the server **24**, to mobile network operator **18** to end user **20** on the SMS phone or other type of cellular device. Similarly, user **16** may send a message via a (Mobile Originating) MO SMS phone to an end user **20** on the SMS phone through a similar path through the mobile network operator **26c**, server **24** using the database **22** and then to the mobile network operator **18** which then reaches the SMS phone of the end user **20**.

As illustrated in FIG. **1** with three messaging scenarios, the server **24** is the message broker. The incoming and outgoing messaging types may be different or the same. The messaging parts of the three messaging scenarios of FIG. **1** are independent of one another, and logically linked via the database.

It should be noted that as described in this application, "cellular" or "cell phone" may imply any type of a device, such as a mobile device, with messaging capabilities. Generally, the mobile device such as a cellular phone, pager, wireless hand-held organizer and the like may be used as a point of origination or termination with regard to message sending and receiving. In other words, such a device may be used in sending a message, such as from users **12**, **14** and **16**, and also as a device for receiving a message, such as by user **20**. Generally, the device may refer to a cellular phone using cellular telephony, paging, wireless hand-held organizers and any other such mobile, radio frequency connected numeric or other type of alpha numeric display device. Generally, as known to those skilled in the art, SMS uses capacity in a data channel of digital mobile equipment to transmit text and binary messages to subscriber cell phones or pagers. In other words, a subscriber may use a cell phone or pager to receive a message, for example, as indicated by user **20** in the system **10** of FIG. **1**.

SMS connectivity and SMSCs may comply with any singular standard. Compatibility may be achieved normally only within a single digital mobile network. For example, Global System for Mobile Communications (GSM) is an example of an SMS implementation in which GSM is principally found in Europe and generally employed by a

4

plurality of different digital mobile networks. Thus, sending messages in SMS format between digital mobile networks, for example, in Europe is more unified. A sender and a receiver may communicate with less difficulty, for example, in Europe than in another region such as North or South America, where there may be a higher occurrence of mixed technology of digital mobile networks, for example, such as AMPS, TDMA, CDMA and GSM. Additionally, SMSC manufacturers are diverse each with their own protocol which may also cause problems in communicating between different networks.

The WAP is one of a variety of cellular phone based microbrowser technologies permitting the user to be able to access traditional and modified content and applications from the Internet, as shown, for example, in the system **10** of FIG. **1**. It is understood that WAP is used herein as an example of a mobile device with browser. The device may comply with various standards as may be used in connection with a mobile browser device, such as a I-mode handset, or Wireless PDA with proprietary micro browser, and the like.

As will be described in paragraphs that follow, and with reference to the system **10** of FIG. **1**, the techniques described herein may be used to unite different platforms, messaging formats, geographic locations, cellular technologies and/or messaging types using a common point of entry exchange and application with transparency and seamless message sending to the sender and one or more message recipients.

For example, as described in paragraphs that follow, FIG. **1** shows a system **10** which may be used in connection with sending and receiving a message on two different digital mobile network, such as Voicestream and AT&T Wireless.

Short messaging as may be used in connection with SMS generally involves the transmission of short, text and/or numeric messages, between a message handling system and a mobile subscriber. For example, a message may be up to 140 octets carrying up to 160 characters of text. In some systems, short messages may be used, for example, in connection with paging. Applications, such as those that obtain stock quotations, weather and traffic and news information as well as sports broadcasting information, may also use a short message to transmit information in connection with these applications. For example, if a user wants to know what the weather is in a particular city, a subscriber of a particular digital mobile network may contact or send a message to the cellular operator of the network. In return, the particular user may receive a short message describing the weather associated with the city of interest specified in the previous request.

As may be known, for example, in connection with the use of digital mobile networks but omitted from the system **10** of FIG. **1** for the sake of simplicity, each SMS message may be routed through the mobile network, between base stations, main switches and then short message service centers or SMSCs. Referring to the system **10** of FIG. **1**, SMSCs, for example, may be cellular operators **18** and **26c**. The SMSCs may optionally offer connectivity to other external sources in addition to messaging services within the individual mobile network operators closed network.

Short messages may be sent from a first, sending user, such as user **12**, to end user **20** as may defined in accordance with the database **22**. The sender of a message may identify a destination associate with an end user, a corresponding device, and a user's mobile identification number (MIN) or phone number.

It should be noted that although FIG. **1**, **1A** and other may show a connection medium as being the internet or WWW



## US 7,209,950 B2

5

and associated HTTP protocol and standard, it should not be construed as a limitation. Other connectivity options are possible as described in more detail elsewhere herein.

Referring now to FIG. 1A, shown is an example of another embodiment of a portion of the network 10 of FIG. 1. Generally, FIG. 1A shows a more detailed description of the components previously included in FIG. 1. FIG. 1A additionally includes detail regarding particular hardware that may be included in the network 10. The particular hardware, may be, for example, owned or leased by a particular digital mobile network to provide services therein.

In particular, FIG. 1A shows more detail of one representation of how messages may be routed within a particular cellular network. It should be noted that the rearrangement of the components does not functionality different from that previously described in connection with FIG. 1. In other words, for example, the functionalities as described in connection with FIG. 1 also apply to FIG. 1A in which two-way communications or bidirectional communications may occur between two different users such as 50a and 50b in different networks such as cellular network A and B, respectively. Messages between these two users in two different networks may be made possible through the server 24 and the database 22.

In the arrangement shown in FIG. 1A, a message may be sent from a first user with a cell phone 50a to a second user, for example, having a cell phone 50b. User on cell phone 50a is included in cellular network A, and user on cell phone 50b is included cellular network B. The SMS message, for example, from the device 50a may be routed through the cellular operator A's network. An SMS message originating from the device of user 50a, for example, may be transmitted to the radio tower 48a, to base station 46a, through the master switch 44a and the SMSC 43a to the SMPT gateway 42a using the worldwide web (WWW) 40a.

From this connection, the message may be routed to the server 24 to obtain information for appropriately routing the message using the database 22. The server 24 then forwards the message using the web 40b, for example, to the web SMS application 42b as operated within the cellular network B. The message is further forwarded through components, such as the SMSC 43 being the master switch 44b of the cellular network B. Finally, the message may be sent to a base station 46b, and radio tower 48b to reach the device 50b which is capable of receiving the message as sent from the device of the user 50a.

Within the arrangements, for example, shown in FIGS. 1 and 1A, short messages may be received by the server 24 and forwarded to one or more end user in accordance with the SMSC database that includes addressing and messaging format information customized for each particular digital mobile network to which the server 24 is connected. The central routing server 24 includes detailed information about a each mobile network operator, such as:

- Routing method and path
- Maximum message length
- Device type
- And also User information, such as:
- Device type
- Account status
- Billing information and privileges

With the information, the central server 24 may forward the message in the correct way for the recipient. For example, if a sender's SMS message is 160 characters long but the receiver's SMS messaging system only supports 120 characters, the message is split in to two portions before forwarding, i.e. 1/2 and 2/2. By means of another example:

6

the sender's account may also be consolidated with the SMS usage by providing confirmations of successful message reception back from the recipient.

The forwarding destination may be defined by the MIN or phone number of a particular cellular user. Since the SMSC is connected directly to the master switch and informed by the home location register (HLR) that functions as a part of the master switch as seen in elements 46a, b and c on FIG. 1A. of the cellular phone user's presence on the network, messages may forwarded to the cell phone, for example, when it is switched on. Otherwise, messages may not be immediately delivered and may be accordingly held in storage for a predefined period of time. If these messages, for example, in a particular digital mobile network, are not delivered to a particular user after a predefined period of time, they may be deleted. These messages may be stored upon a computer storage medium, for example, that may be included in the SMSC of a particular user's digital mobile network.

An SMSC, for example, referring to 18 and 26c as shown in FIG. 1 and elements 43a through 43c of FIG. 1A, may receive alpha numeric messages from other cellular subscribers or from external sources. This may be, for example, in connection with mobile originating devices or two-way SMS communication devices.

The mobile network operator may use one of several different types of techniques to enable communications between users on the same or different networks. These different techniques or methods may be chosen, for example, in accordance with the source and destination characteristics for the message. Note that the following that will be described are techniques that may be used in connection with forwarding an SMS message from one digital mobile network to a destination digital mobile network.

Messages may be received by a user, for example, in connection with voice phone calls that are forwarded by an operator that may be at the SMSC. The operator may manually type in the message via a remote terminal connected to the SMSC which may then be forwarded to the destination user. As an example, someone may leave a voicemail message for the user 20. Rather than have a first user send an e-mail or other type of text message directly, the first user may speak with an operator who transcribes the message from a remote terminal connected to the SMSC. Other techniques may be used in connection with transforming a voice communication to a written electronic communication, for example, using software and/or hardware that automatically converts a voice communication to an electronic communication, such as an e-mail message. This message may then be relayed to the end user's cellular device from the SMSC, for example, such as between 18 and 20 referring to the system 10 of FIG. 1.

Messages may also be entered via a remote terminal of the SMSC using a web page associated with a particular cellular operator/network. In one example, the SMS message forwarded to the user is within a particular digital mobile network and data may be entered using the web such as 26a as a connection. A user such as 12 referring to the system 10 of FIG. 1 may enter information into a web page serving as a data form. A message is produced in accordance with data entered into the web page, and then forwarded to a destination which may be within the same digital mobile network. This data form as a web page may be used by a user sending a message from any one of a variety of communication devices, such as, for example, a hand-held device,

cellular telephone, or terminal connected to a system capable of communications in accordance with the HTTP message protocol.

SMTP gateways, such as used for sending standardized e-mail messages, may be enabled at the SMSC allowing e-mails to be converted into SMS messages. This may be shown, for example, with reference to FIG. 1A, network 60, cellular operator A in which the SMTP gateway 42a may be used, for example, to convert a received or incoming e-mail message in the Digital mobile network A sent from a user on another system into an SMS format that may be displayed, for example, on the user's device 50a. In this example, the e-mail may be addressed to the user's MIN or phone number at the cellular operator's URL. For example, to send an SMS message to Bob whose cell phone number is 23674 on network X, the e-mail may be sent to 23674@networkx.com. The e-mail subject text and message body may be sent as the SMS message content. This will be described in more detail in paragraphs that follow.

Messages may also be sent to an SMSC using a software program, such as 42b, that format incoming messages according to the type of format of a receiving SMSC. Connection mediums that may be used are diverse data transport systems including, for example, modems, ISDN, frame relay, X.25 packet switch networks, or TCP/IP. This may be illustrated, for example, with reference to the network 60 of FIG. 1A, cellular operator C using the direct SMSC connection 42c, the SMSC 43C to perform any translation or reformatting of data necessary to further relay an incoming message in the form of an SMS message format to the user 50c.

Messages and commands may originate from devices with mobile origination (MO) device capacity. This may be routed to a particular SMSC from a device's "home" or originating SMSC.

The mobile network operator of one or more digital mobile networks as previously explained may use any of the foregoing techniques as well as others to enable communications between users in the same or different networks. End point users may be identified, for example, by a MIN or phone number included, for example, in the message entered via the web page, or e-mail, or other type of communication which is converted to an SMS format.

Generally, a sending user may associate a name and a phone number or MIN, for example, as identifying indicia of an end point or end user who is the target recipient of a message. Users may not be concerned with details relating to the formatting of each particular network and may rather have the details appear "invisible" by a seamless transfer of a message between users within the same and/or different networks. Using techniques that are described herein, the process of forwarding messages from any one of a variety of these different sources to a particular user of a network regardless of whether the networks are the same or that they are different networks having different protocols and other types of incompatibilities may be streamlined.

As described herein, users of different or the same networks may be provided with services for streamlining SMS based messaging services. Mobile originating SMS messages may pass from one device to another regardless of the operator, location or network technology. To simplify the messaging process, mapping or translation of the different formats in accordance with the different sources and destinations, hardware and protocol differences are accounted for and handled by the server using a routing database. Thus, users are not encumbered by the details of the different types of connections facilitating a smooth transition of messages

between different networks which may otherwise be incapable in accordance with different formats and protocols and the like.

Referring back to FIG. 1, the user 12 may use a personal computer that is capable of reading HTML. The terminal may further be connected to the WWW using HTTP protocol format for connecting to the server 24. The user 14 may have a wireless access protocol (WAP) phone or other WAP device capable of understanding the wireless mark-up language (WML) and may communicate with the server 24 in accordance with the HTTP protocol.

Generally, there are different scenarios for messaging which involve one-way as well as bi-directional or two way communications between users. As described elsewhere herein, communications may occur between a cell phone and the server 24, such as the TIAXA server. As an example of a one-way communication, a user may enter information that is sent to the TIAXA server, for example, in connection with entering database information. The database information may be information identifying the sending user, or one or more end users. The entry, for example, may be from a personal computer, may use the web or from a cell phone.

A second type of one-way messaging involves information "pull" between a cell phone or user of a digital mobile network and the server, for example, for inquiries such as about the weather in Miami.

A third type of service provided within or between digital mobile networks involves a relay servicing of messages. For example, a user may contact one or more other users through the server 24 used as a "hub". Referring to FIG. 1 as described elsewhere herein, user 12, for example, may communicate through the server 24 to an end point such as 20. Additionally, a user may forward an SMS message, for example, having multiple end points rather than a single destination.

The server 24 may account for, and facilitate communications between, all combinations of connection types and format cases using the different type of sources for message creation as well as destination in order to map an incoming message to a target. The server 24 may also be used, for example, as a broker, translator or reformatter that has "embedded" knowledge of the source and targets that are possible for the different types of networks. The different formats and the mappings may be performed, for example, using software executing in the server 24 using information stored in the database 22. This type of transaction or mapping may be provided for a streamline appearance to a user in sending a message, for example, on one digital mobile network to another user on another digital mobile network, each having different formats and protocols.

Shown in a table below are the different types of SMSC connectivity options, for example, as may be represented as the connection between the server 24 and each of the SMSC cellular operators such as 26c and 18 referring to the system 10 of FIG. 1.

TABLE 1

SMSC Connectivity Options		
SMSC Manufacturer	Protocol	Transport
Logica	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Lucent	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP

US 7,209,950 B2

9

TABLE 1-continued

SMSC Connectivity Options		
SMSC Manufacturer	Protocol	Transport
Motorola	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Sema	OIS, SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
ADC	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Newnet		
Comverse	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Ericsson	SMPP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
MXE		
CMG	UCP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Nokia	CIMD2, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP
Generic/Open	TAP, SMPT (email), HTTP	modem, ISDN, X.25, X.31, TCP/IP

The foregoing table summarizes for each of the different types of SMSC hardware manufacturers the different protocol as well as transport medium that may be used in one particular embodiment at a particular point in time. As additional digital mobile networks, or spokes, are added in connection with the hub (server **24** and database **22**), additional protocols, and the like may be added to the above table. It should be noted that the protocol described in column **2** above may represent the communication protocol, for example, used at links **25a** and **25b** between different SMSC operators and the server **24**.

It should also be noted as described in more detail elsewhere herein, the information regarding the protocol and transport medium may be encoded in the database **22** in one or more fields.

As also described herein in one embodiment, the point of entry of a user may be defined as a the web server which is accessible using the internet via a PC, a microbrowser enabled phone with internet capabilities, or through a mobile originating (MO) mobile device such as a cell phone.

It should also be noted that the server **24** in one embodiment hosts the software web pages in the link needed to perform and implement the foregoing techniques. The front end interface, for example, as may be used to display information and the users PC **12** be written using standard internet protocols allowing the user to send SMS messages. The database is described in more detail elsewhere herein and may use any one or more of a variety of commercially available packages, for example, such as may be available from vendors Oracle and/or Sequel.

The hardware of the server **24** may be any one of a variety commercially available hardware processors that may vary in accordance with the traffic the server is handling. In one embodiment, the software that executes on a server **24**, for example, may be Windows NT using Sequel, the LINUX operating system, or other UNIX-based operating system using an Oracle database. It should be noted that embodiment may include any combination of hardware and/or software in accordance with the traffic and other types of parameters within a particular system.

Since a variety of different devices may be used to interface to the server **24**, different types of user interfaces may have to be tailored or targeted for a particular device. In accordance with standard protocols, different devices may be identified, for example, in incoming messages to the server as part of the message format. This information may

10

be used, for example, to display device specific information. Selection of a particular format and data sent to a particular device may be made by the server **24** in accordance with received device-specific information.

Referring now to FIG. **2**, shown is a flowchart of steps of one embodiment from a user-interaction perspective for sending an SMS message. In this example, these steps described are those that may be associated with using the WWW or the internet for sending a message. The steps that will be described in conjunction with FIG. **2**, flowchart **70**, are those that may be performed when an SMS message is originated from the web, as illustrated by elements **12** and the **14** of FIG. **1**.

As described in more detail below, a user may use and access the server **24** and database **22** through the Internet using, for example, a personal computer, microbrowser or any other device providing for interaction with the server **24** of the message delivery system. The user may then register and/or send messages using the server **24**. A web page may be displayed to a user in connection with entering message information. Generally, the embodiment described herein may use the routing database to perform queries, for example, to obtain a country specific format of an associated mobile identification number (MIN) when sending a message and/or during registration of a user of the server **24**. The routing database may also be queried in connection with determining the existence of a particular user's MIN for an associated country, for example, as may be performed in connection with "sending" a message. Additionally, the routing database may also be queried.

At step **72**, the user enters the URL of the website or webpage from the user's device. This URL may be the address of a website and result in a webpage being transmitted and displayed to the user. The user may enter this information, for example, from a personal computer, a wireless access protocol, or "WAP" phone, or other device having internet capabilities. In both of these instances, there may be software and/or hardware associated with the originating device for processing HTML files in accordance with http protocol, for example, such as those included in a browser, and may reside, for example, in a personal computer.

At step **72**, the user enters the address of the home page **74** as indicated in the flowchart of FIG. **2**. Control proceeds to step **76** where a determination is made as to whether the user is registered. If a determination is made that the user is not registered, control proceeds to step **78** where a user registration process may be performed. For example, a registration process may be performed to register a user, such as **12** or **14** with reference to FIG. **1** using the server **24**. This registration process enables the user to send a message, for example, to another user at a different network using the server.

If a determination is made at step **76** that the user is already registered, control proceeds to step **80** where the user sends a message page. As part of the message-sending process, Field **81** outlines those portions of information which may be entered, for example, interactively through a user interface or form display with a web page. As shown at **81**, the type of information entered for sending a message may include the user's name, a recipient's name and a recipient's country. Note that if the international number form is used, the recipient's country is not needed. The user's name, the recipient's name, and recipient's country may be, for example, alphanumeric characters. Values associated with these items may be input using forms or web pages written, for example, using HTML processing as



US 7,209,950 B2

11

interpreted by a browser and may interpreted on an originating message-sender's device, such as a personal computer in connection with sending a message from user's computer 12 or from a particular type of WAP phone 14 capable of interpreting a form of HTML, such as WML.

At step 82, the routing database 22 may be consulted to obtain the country number format. In response to the user selecting the SMS recipient's country as entered at step 81, the database may be consulted to return the correct MIN numbering format as an input example. This may be displayed at step 84 as one of the fields to the sending user. Referring to FIG. 2, flowchart 70, step 84 indicates a field 84a which may be output or displayed, for example, on the user's screen to guide completion of a subsequent field 84b. These help guides may vary with each country and may be returned by the database shown in FIG. 8, for example in field 410. The help guides may include an example of the required MIN format and a short help text in the appropriate language. Additional fields, for example, may be included in a form in which users enter the data of 84b for the recipient's phone number following the same format specified in 84a as well as the message text in field 84c.

Subsequent to completing processing at this point, the message 84c as well as the recipient's phone number 84b has been entered. At step 86, the message is sent to the server 24 along with the additional information input as the recipient's phone number. At step 88, the routing database 22 is consulted for the recipient's phone number. In other words, the routing is queried as to the existence or entry of the recipient's phone number within the routing database 22.

At step 90, a determination is made as to whether this number has been found within the database. If a determination is made at step 90 that the recipient's phone number is not within the routing database 22, an error message may be generated, for example, in the form of an HTML page to display the message to the user at step 106. Control returns to display the home page 74 on the user's internet device. The steps in connection with obtaining a message to be sent are started again, for example, by displaying a home page 74.

At step 90, if it is determined that the number is within the database 22, (this information is held in sector 406 of the database shown in FIG. 8, particularly in ranges 406f and g), control proceeds to step 92 where the routing database 22 is queried regarding the required routing message method. The required routing message held in sector 404 of the database shown in FIG. 8. At step 90, if no match is found for the entered number, an error is generated 106 advising the sender that the recipient's number does not exist as in 104. At step 92, if no routing method is found 94, the sender is advised at 102 of the lack of routing path to his recipient as in 104.

At step 94, with the routing determination obtained in the previous step 92, it is known which type of message delivery formats will be utilized for the particular type of network, its protocol and the like in accordance with the recipient's information. If the routing information is known at step 94, control proceeds to step 96 where the message is placed in the appropriate format and sent in accordance with the information returned at step 92 for the particular routing technique. In other words, the data input by the user, for example, as part of the input processing at step 84, such as the message content 84c and the recipient's phone number 84b such that the message and other information may be appropriately forwarded to the indicated recipient in accordance with the routing information obtained from the database 22 in processing step 92.

12

The various message types and formatting are described in more detail herein elsewhere in connection with other figures. Additionally, it should be noted that other processing may be performed in connection with step 96, such as performing a mail "spamming" check or other types security and filtering of messages sent, such as the elimination of offensive text with filters and the like. Software used in connection with such functionality, for example, may be stored and executed on the server 24. The message is formatted in accordance with, in this example, different types such as the SMTP message type 108a, the web posting application format 108b, or a direct SMS connection message format 108c. Upon reaching this point in processing, control proceeds to step 98 where a message may be displayed upon the sender's device indicating that the message has been successfully sent.

If at step 94 a determination is made that the routing information is not known, control proceeds to step 102 where an error message may be generated and displayed on the user's device, for example, in the form of an HTML page that is processed by the browser, for example, residing on a user's personal computer. The message may indicate, for example, that the recipient's mobile network operator has not enabled messaging services. At this point, processing may return to displaying the home page 74 and beginning the processing of entering a new recipient or recipients.

It should be noted that what has been described in connection with the flowchart 70 of FIG. 2 is a process that may be generalized for sending more than one message to more than one recipient on different networks. Additionally, it should be noted that the initial query performed at step 82 may also be used during the registration process or as part of editing or adding a new mobile device. For example, the user may be required to enter a country as well as a phone number or MIN. The database may be consulted, and the correct country-wide MIN may be returned to the user to serve as a template for user entry in connection with user registration.

Users of a server based system as shown in FIG. 1 may be required to register before hand. There are some services that are offered for technical or commercial reasons that may not require registration. A registered user may be added to a database that works in the central server and routing database 22 and 24 respectively. By registering, the user allows the server knowledge of his mobile device and other such information that permits an optimization of messaging to and from the user. Another application known as an "Address Book" or "Buddy List" allows the user to add information about people who are frequently used messaging partners. Such address book would typically contain the friends phone number, associated routing path, and name. The registration process may use a collection of data, and assignment of passwords and privileges etc.

It should also be noted that the processing of FIG. 2 includes steps that may be used, for example, where an originating device has internet or browser capabilities, such as a browser phone or personal computer or other device that may transmit data in accordance with HTTP protocol in this example. Part of the processing steps of FIG. 2 may transmit data interactively, or in real-time session.

Referring now to FIG. 3, shown is a flowchart 120 of method steps of one embodiment that may be used in performing communications, for example, originating from an MO SMS phone 16 with reference to the network 10 of FIG. 1. It should be noted that the processing steps of FIG.

## US 7,209,950 B2

13

3 may not be performed in real time, but, rather, using an SMS data channel for message sending from the MO SMS device 16.

Processing begins with the user utilizing an MO SMS device to generate messages or to “pull” content, for example, from a web page of another server or other information/data source. The messages may be generated, for example, using input from 122a and 122b (as examples of simple messaging using SMS, as well as the example shown in 122c, to pull “content” from server 24, or any other appropriate external server connected through server 24. The input at 122a is directed to a recipient that is not in a buddy list. Generally, a buddy list refers to the concept of a list of commonly used names or recipients, for example, that may be buddies to which a sender may commonly send messages. The “buddy” recipients may be included in a short list, or buddy list rather than go through a process of consulting the database for complete information.

At step 122a, one type of SMS message may be sent to a recipient who is not in a sender’s buddy list. At step 122b, an SMS message may be directed to a recipient who is in a sender’s buddy list. At step 122c, a message may be sent using an SMS message, for example, to pull “content”. In other words, the message includes data such as 122c that includes stock information which is to be returned in the form of a SMS message to the sender. In this example, the server may poll the host SMSC such as 26c at certain predetermined time intervals to retrieve SMS messages as may be forwarded, for example, from the MO SMS device 16. This processing may occur, for example, as part of step 124 where the sender may form the message such as 122a and forward this to the cellular operator 26c.

There are two basic methods for receiving messages from non-browser mobile devices such as MO SMS cell phones:

1. As email—Most MO SMS phones have the ability to send Email, these emails are sent as SMS to the host networks SMSC and there the full SMTP format is completed. This SMTP format may add the sender’s return email as MIN@operator domain format, for example 2322332@operator.ext. In this case, the receiver of these emails may use a POP3 email server, hence is “received in email form” as indicated in step 124 of FIG. 3. The POP3 email server may be associated with the central server 24 of FIG. 1. The POP3 server may also be remote.
2. As MO SMS—If the message is written as a MO SMS, it is to a given number. This number may be a short number (assigned by the network operator for example “8200”) or a normal MIN number such as “5693183098”. The first case may be more common. Once sent, this message is received on the host networks SMSC. Upon reception at the SMSC, the message is placed in an outgoing spool file. In the example shown in FIG. 1, the central server 24, may poll the SMSC 26c via the dedicated connection 25b, collecting messages destined for the server 24.

The SMSC 26c may associate the server 24 by the short number as described above.

In either of the two cases described above, the message is received as a formatted text file. This is the file that is received on the server 24, and represented by step 128 of FIG. 3. In step 128 parsing logic isolates required fields from the received text files and searches for commands, such as “STOCK”, seen in 122c, and “Soames”, seen in step 122a. The former is a request for a stock quote, and the latter relates to a “buddy” in the user’s address book called “Soames”.

14

Using the steps described in connection with flowchart 120, a user, for example, may enter a request to “pull” data from another web site or server. The server 24 forwards the desired information, content, or application requested to the device of the requester, and/or sends a message to another enabled device.

At step 128, the SMS message is received and parsed. In particular, the sender’s mobile number is extracted from the SMS message. It should be noted that prior to being received at the server 24, the SMSC may tag incoming SMS messages with the originator’s or sender’s phone number (MIN). Similarly, incoming e-mail messages may be tagged with the sender’s return e-mail address. These fields may be used in cross-checking an existing user database, for example, that may be stored, for example, in the database 22.

The user database is linked to the routing database 22 as described elsewhere herein. Step 130 compares information included in the incoming message to that from a database. For example, user identification (usually recovered MIN number) and keywords may; be compared to the parsed message from step 128. The keywords have a standard form, and alternate or “acceptable forms”. The keywords have two forms:

1. Static Keywords: For example, in connection with 122c, the standard form of the keyword is “STOCK” but the acceptable forms may be many, for example, such as, “stock” (lower case), “share”, “shareprice”, “stockprice”, etc. These keywords may be common to all users.
2. Dynamic Keywords: For example in connection with 122b, “Soames” is a name from a user’s buddy list. The dynamic keywords are loaded each time the user is recognized as originator of the message.

At step 130, this database may be queried or consulted to determine if a particular user is registered in accordance with the MIN extracted from the SMS message at step 128. Registered and unregistered users may have varying privileges in accordance with actions that may be performed in sending messages to other recipients of this network as well as other networks. At step 132, a determination is made as to whether a sender is registered in accordance with this MIN.

As some operators choose not to disclose their user’s MINs when forwarding messages, the authentication may also be performed on user “alias” names. For example, instead of forwarding the users MIN and operator extension such as 123232@operator.ext, the user may assign the user an “alias” such as tomato@operator.ext. In either case, this information is obtained during the registration process, and may be authenticated.

If a determination is made that the sender is not registered, control proceeds to step 134 where a user registration process may begin. It should be noted that subsequent to user registration at step 134, control may resume with processing, for example, at step 136 in connection with sending a message.

Upon determining that a sender is registered at step 132, control proceeds to step 136 where the previous parsing of the SMS message is again compared to a database for keywords to determine if the SMS message includes a phone number. At step 138, the web database is consulted. The user database is linked to the routing database 22 as described previously. Step 138 compares information contained in the incoming message to a database.

At step 140, if it is determined that the received SMS message does not begin with a phone number, control proceeds to step 142. At this point, the message may be an

## US 7,209,950 B2

15

alpha numeric indicator that may be, for example, either a buddy or another keyword command. In the case of a buddy, this buddy has previously been configured in the sender's database. If the recipient is not found in the user's buddy list, control is passed to step 190. Control then proceeds to step 192 where the keyword is compared to existing commands. A keyword determination may indicate, for example, if a particular piece of data is to be polled from the server and sent to the sender or originator, for example, with regard to the stock quote, weather information, and the like.

Note that where referred to herein, "content" refers to "pre-packaged" information such as stock quotes or weather. "Application" refers to a process, for example, generation of a ring tone that is sent back to the user, or participation in a game, in both of which "processing" is required by the application upon the user's input.

If a determination is made at step 192 that the SMS message indicates or includes a keyword, control proceeds to step 194 where the content or the application is returned to the user and control proceeds to step 180 where the message is formatted and sent via the appropriate method. At step 192, if a determination is made that a first identifier in the SMS message is not a keyword, control proceeds to step 186 where a SMS error message may be generated, indicating that the command received is invalid and the message, as illustrated on output element 188, may be displayed.

If at step 182 a buddy's name is found in the user's database (see previous note on "Dynamic Keywords"), the routing path for that buddy is returned and the message is sent 184 to the recipient. As previously described in connection with FIG. 2, steps 196a, 196b and 196c may result in reformatting of a message in accordance with the appropriate format and type for the recipient's network and connection. These are similar to what is described in connection with the processing of steps 108a, 108b and 108c of FIG. 2 and as described elsewhere in connection with FIG. 2.

At step 140, if a determination is made that the SMS message begins with a phone number, control proceeds to step 144, where the SMS message that is received by the server is parsed to extract the recipient's country code. At step 146, this recipient country code is used to look up in the routing database 22 a corresponding country for the country code extracted at step 144. The country codes (prefixes) and numbers may exist in sector 406 of the database shown in FIG. 8. At step 148, a determination is made as to whether the country has been located from the routing database. If a determination is made that the country has not been located, control proceeds to step 150 where an error message is generated and the message is returned to the sender at step 154. As an alternative process, (not shown) logic may be such that in the case of not finding a country code, the recipient is deemed to be in the same country as the sender, in which case the senders country code may be added to the recipients number. More detail of the number lookup process is shown in a detailed flowchart FIG. 4.

If the country is located and determined at step 148 to be included within the routing database 22, control proceeds to step 168, where the SMS message is parsed to extract the recipient's phone number. The routing database 22 may be queried to look up the recipient's phone number. A determination is made at step 172 as to whether the MIN or phone number is located within the routing database. The country codes (prefixes) and MIN numbers may be included in sector 406 of the database shown in FIG. 8. At step 172, if the number is not located within the routing database, control proceeds to step 156, where an error message is

16

generated and control proceeds to step 154, where the SMS message is returned to the sender.

At step 172, if the number is located in the routing database, control proceeds to step 174 where the database is queried for the required routing method in accordance with the recipient's phone number, country code and, accordingly, the appropriate routing techniques used in accordance with the protocol, hardware and the like for the recipient's particular network. At step 176, a determination is made as to whether the routing information is known. If the routing information is known, control proceeds to step 178, where the SMS message is parsed, the message text is extracted from the message and control proceeds to step 178, where the message is formatted and sent via the appropriate method as indicated in accordance with the information from the routing database. Control proceeds to step 164, where an SMS report may be generated, the message may be sent at step 166, and control proceeds to step 154 where a message is returned to the sender indicating the actions taken.

At step 176, if a determination is made that the routing information is not known, an error message may be generated such as indicated at output 162 that the recipient's network operator has not enabled messaging services. Subsequently, from the processing at step 160 that may result, for example, in a display of a message as indicated at 162, control proceeds to step 154 where the SMS message is returned to the sender. As previously described in connection with FIG. 2, steps 196a, 196b and 196c may result in reformatting the message in accordance with the appropriate format and type for the recipient's network and connection. Please note that these are similar to what is described in connection with the processing of steps 108a, 108b and 108c of FIG. 2 and will be described in more detail in paragraphs that follow in connection with other figures.

The processing steps described in connection with flowchart 120 of FIG. 3 are those that may be performed in connection with data polling to obtain information, such as a stock quote, or sending a message to another enabled device where the originating device, for example, may be an MO SMS phone, such as element 16 of FIG. 1. Previously described in connection with FIG. 2, are processing steps that may be associated, for example, with sending an SMS message originating from a personal computer or from a WAP phone as shown with reference to the network 10 of FIG. 1 from elements 12 and/or 14. Using any one or more of elements 12, 14, and 16 of FIG. 1 as points of origination, an SMS message may be sent, for example, to user 20 using the SMS phone through the routing database 22. The database 22 may be queried in accordance with software executing on the server 24 as indicated in connection with various processing steps just described herein.

It should be noted that, with reference to processing steps of flowchart 120, if the SMS message does not start with a number, for example, such as a phone number possibly preceded by a "+" sign with at least eight digits, then the first "word" in a message body may be examined in accordance with a user's buddy list. If the first word is determined as identifying a buddy, the processing of flowchart 120 directly sends this message to the buddy or buddies and the messaging format is already known as they are within the same network. If a determination is made in connection with the processing of step 192 that an incoming SMS message includes a keyword, keywords may be used in an embodiment to abbreviate common commands. For example, as previously described in requesting a stock quote, the user may start an SMS message with the word "STOCK" fol-



US 7,209,950 B2

17

lowed by a ticker name or other type of stock indicator. In this instance, the required information may be retrieved from the server or other servers and returned directly to the sender of the message. Additionally, features within different embodiments may allow the sender to further forward the content or applications to others. For example, a command known in one embodiment as the "RING" command, followed by a phone number, followed by a group indicator may forward one or more RINGING audible tones from a specific group of tones to a particular phone number indicating a recipient.

In general, from the above description, and the logic of FIG. 3, it may be seen that certain services, that are those that are thought to have higher volume of use, may be given higher priority in the logical process sequence. The presented priority is one example, and may change as user needs change. The presented priority is:

1. Messaging to a phone number
2. Messaging to a pre-configured "buddy"
3. Messages requesting and application or content

It should be noted that in processing an SMS message, if the SMS message is preceded with a number, for example, that may indicate a MIN or phone number, that MIN or phone number is parsed and checked in the number routing database 22. This MIN or phone number may include, for example, a country code. Some countries, such as the United States, may have only a single digit, such as a "1," to indicate the country code. The parsing and checking processing of the phone number may be performed for each single digit until a unique match for a country code is found.

For example, if a message recipient's phone number is indicated by the string "+5693183098", the 5 at beginning of the string may first be checked in determining the country code. As a result of querying the database, there may be an indication that there are multiple country codes beginning with a leading digit of "5". Thus, a single country is not unique for the digit five. A subsequent second look-up may be done upon the same string returning a "6" as a second digit. Thus, a database query may be performed using five six "56" as the country code. Upon a single country being returned as result of a database query, the "56" indicates a unique combination of two digits corresponding to a country. For example, in one embodiment, performing a query of routing database for the one or more countries having a country code with first two digits of "56" returns the single country of Chile. The return of only a single country being associated with the two digits causes the country-code look-up process to terminate. If no country is found, an error may be generated for example in connection with the termination processing at step 148 and the error message 152 displayed in connection with the processing of step 150 with reference to flowchart 120 in FIG. 3.

It should be noted that the foregoing search for a unique combination of one or more leading digits of a country code may iteratively be performed examining each next digit until a unique country is associated with the number of digits, or no such country has been determined to include those as leading country code digits.

Once a valid country code has been identified the remainder of the recipient's phone number may be examined. An additional query may be performed in the routing database to look up the remaining portion of the phone number only in the predetermined country, for example, such as Chile in accordance with the country code just examined. If this phone number of a recipient is not located within the country corresponding to the country code, an error message may be generated. This is an example of processing that may be

18

performed in connection with step 170 and the determination made at step 172 in which the database may be queried for a particular phone number in accordance with a particular country code. Accordingly, an error message at step 156 may be generated if the particular phone number is not in existence in the database where the predetermined country as entered by the country code.

Referring now to FIG. 4, shown is a flowchart 200 of steps of one embodiment for performing a look-up in the routing database 22. The steps in flowchart 200 may be performed, for example, in connection with consulting or querying a routing database to return particular information. Generally, the processing described in the flowchart 200 of FIG. 4 details database querying steps, for example, as previously described in connection with flowcharts 120 and 70.

A recipient's phone number and message for example may be entered using any one or more of a variety of different types of devices. Input may be received 202 using the internet or WAP device as well as from an MO SMS phone 206. In both instances, data input may indicate a message, and a recipient's phone number as indicated in input 204. Control proceeds to step 208 where the first most significant digit is parsed or selected from the string identified as the recipient's phone number in the message. Beginning with step 208 processing, a determination is made as to the particular country code indicated in the recipient's phone number. In step 210, the routing database 22 is queried to return a list of countries having the first most significant digit as parsed at step 208. In this example, "1" may be the most significant digit in accordance with the sample input at step 204. If no country codes are determined at step 212 to include a "1" as the leading and most significant digit, an error message may be returned as part of the processing at step 214.

Otherwise, if there is a "1" that is the most significant digit in one or more country codes as indicated in the routing database, control proceeds to step 216 where a determination is further made as to whether there is only a single instance of a country code having a most significant digit of "1". If there is a determination made that there is more than a single instance of a country code having a most significant digit of one at step 216, control proceeds to step 236 where a combination of the current first most significant digit followed by the second most significant digit is extracted or parsed from the phone number and the database is then consulted at step 238. The foregoing general processing of determining if there is a unique country code having the current set of significant parsed or extracted digits is repeated at step 240 where a determination is made as to whether there are any country codes having the combination of the first and second most significant digits.

An error message is returned at step 242 if a determination is made at step 240 that there are no such country codes valid in accordance with the routing database. Otherwise, control proceeds to step 246 where a determination is made as to whether there is only one instance of a particular country code indicated by the processing of the combination of the first and second most significant digits. This process may be generalized and repeated for a combination of significant digits until only a single country code is found and matched to a particular combination of most significant digits from the phone number.

Upon finding a unique country code for a combination of one or more significant digits in the recipient's phone number, control proceeds to step 218 where the corresponding country code is returned. Subsequently, the remaining portion of the recipient's phone number is looked up in the



US 7,209,950 B2

19

routing database **220**. In other words, a query of the routing database may be performed to determine if, for the particular unique country code, is the individual recipients' phone number included in the routing database.

Upon reaching processing at step **222**, a unique country code is determined and a the routing database has been queried as to the existence of the recipient's phone number in the country indicated by the unique country code.

Associated with step **224** is yet another technique that may be used in determining a country code. Other processing steps described herein in connection with flowchart **200** extract a country code and determine a unique country code from input in accordance with a parsing technique using a unique combination of leading digits as recorded in the routine database. At step **224**, a country code may also be selected, for example, from a pull-down menu causing the associated country code to be an input to the system in accordance with a menu selection.

In either of the two cases, at step **220**, the now known country code is ignored and the MIN number ranges for that defined country are queried in accordance with the recipient's number's ("MIN look up"). For example, if the country code was found to be "one" either by the iterative process, or by direct user selection, the MIN lookup is performed only within the USA portion of the database. The lookup is performed in step **222**.

If a determination is made at step **222** that the recipient's phone number is not within the range valid for the particular country code, control proceeds to step **226** where an error message is generated indicating that the recipient's phone number is not in the system.

If a determination is made at step **222** that the recipient's phone number is within the range of valid phone numbers returned at step **220**, control proceeds to step **228** where a query or a determination is made as to a particular messaging format being defined for the returned mobile network operator and the message code. In other words, a determination is made in step **228** whether the format is defined or known for the particular network supporting the user or recipient having the phone number entered at step **202** or **206**.

If a determination is made at step **228** that the recipient's MIN or cellular phone number is known, but no messaging format is defined for the particular phone number and associated digital mobile network for messaging, an error message is returned at step **230** indicating that the recipient's mobile network operator has not enabled messaging services. Otherwise, if the messaging format is defined for the particular mobile network operator at step **228**, control proceeds to step **232** where the messaging type is returned from the database. Control proceeds to step **234** where the message text address and the like are formatted in accordance with "message code" and "stuff code" fields returned from the database.

It should be noted that particular error messages and the particular fields included in a database indicating the appropriate messaging formats may vary in accordance with each embodiment. A representation of how data may be organized and stored in one embodiment of the routing database is described elsewhere herein. A variety of different data organizations and hierarchical representations of data may be included in an embodiment. Generally, the routing database includes information indicating the different protocol and hardware information for appropriately formatting an incoming message for the one or more recipients in one or more corresponding digital mobile networks.

20

Referring now to FIG. **5**, shown is an example of a representation of a reformatting or a translation process that may be used in sending an SMS message via SMTP email. In other words, as shown in the representation of the mapping **300**, a message format **302** is mapped as indicated by arrow **310** to a new format for message **304**. The text fields input to the messenger's front-end view via a browser are translated or mapped into an SMT TP email format in the background processes described below. The term "background process" refers to a common application, not forming part of this patent claim, typically following an already well-known and used standard. In this case SMTP is the standard formatting method used for outgoing email messages.

It should be noted that the data input in accordance with the format described **302** may be input, for example, from an interface via a web page. It should also be noted that the SMTP format is one example of an email message format in accordance with an email protocol. Different protocol may vary in accordance with SMSC manufacturers as described elsewhere herein.

The recipient's country code is data input in field **306c** may be pre-selected from a pull-down list, for example, from a graphical user interface display. Additionally, the recipient's name may be entered in a field through a form interface **306b** as well as the particular user's name. The user's name **306a** may indicate the sender of the message entered. As described elsewhere herein, in accordance with the recipient's country code **306c**, a sample, or template of a formatted phone number may be returned from the database and displayed in a field **308a**. Accordingly, a user sending a message may input in a field **308b** the recipient's MIN or phone number in addition to the message text respectively in fields **308b** **308c**.

The routing database **22** may be queried using as an input the recipient's phone number or MIN **308b** to return the corresponding mobile network operator and associated routing information for the particular MIN. Routing information may include, for example, a particular protocol, hardware and/or software information regarding how a message is routed, reformatted, and the like for use in a receiving digital mobile network. In this example shown in the representation **300**, the database query when the input is the recipient's phone number **308b** indicates that the forwarding method for that particular carrier network is via SMTP email. For example, the MIN or phone number "305-588-2909" may select AT&T as the carrier for a country code of "1" indicating the United States. Additionally, the returned SMTP address may indicate a format of "mobile.att.net".

The recipient's MIN or number **308b** is then transformed from a countrywide MIN format into that particular format of the mobile network operator. For example, digits may be added or padded or removed from a phone number in order to comply with the mobile network operator messaging MIN or phone number format. For example, a user may input a countrywide format indicated of "3055882909" as returned as user help file for the USA, for example, as included in FIG. **8** sectors **410d** (with text in **410e**, *f* or *g* depending on the users chosen language). The routing database of FIG. **8** returns the exact mobile network operator corresponding to that MIN, and therefore returns the required formatting information. Specifically, the MIN is sought between the ranges **406f** and **406g**, and the formatting information is returned for the located operator **406a** in **402b** and **408a**. For example, what is returned may indicate that the uniform countrywide MIN format input may require further tailoring or modifications to transform this into the proper format to

## US 7,209,950 B2

21

be used in accordance with the AT&T carrier network using the SMTP email protocol. The routing database may indicate that carrier AT&T requires a fixed 11 digit number format and since this is the United States, the country code or leading digit of "1" may be inserted, i.e., "13055882909", as may be returned by 402b. The component of the recipient's phone number 314a which is the reformatted version of 308b is "13055882909" with the @ and the email format for the particular carrier 314b from the routing database, from 404c. In this instance, for example the complete email address formed by combining fields 314a, 314b and the @t sign may indicate an email address of: 13055882909@mobile.att.net.

What will now be described are other types of formatting represented in the FIG. 300. The user's name 306a may be placed in a corresponding field in the SMTP email 304 in field 320b. The recipient's name 306b may be in the destination field 312. Similarly, the subject field 318 maybe some fixed format such as "from Tiixa" or some specified title or application name as indicated in field 318. The message text 308c occupies field 320a of the reformatted message 304.

Optional processing may also be performed, for example, to scan the email or body of the text filtering out predetermined offensive text and the like. Accordingly, the message may be sent and received by the network operator's SMTP gateway such as 42a, referring back to the network system 60 of FIG. 1A. In this instance, the recipient may be user 50a. The SMS messages received as just described by the SMTP gateway, may be translated, and passed to the SMSC to the recipient. The recipient receives the message on the mobile device and accordingly may be processed by reading the message, saving it, deleting it or replying to it in accordance with the device and network type.

Referring now to FIG. 6, shown is an example of a representation of a mapping process that may be performed for a sent SMS message, for example, input from a user interface via the internet to a recipient on a network that uses existing Web SMS applications.

In connection with the method illustrated in FIG. 6, the server 24 writes to the target mobile operators web based SMS interface. The connection from the server 24 to the Web based interface may be a standard Internet, using http over an IP network. The sender of the message, in connecting two the server 24 can use any of the methods and devices shown on FIG. 1, users 12, 14 and 16.

It should be noted that in connection with all three messaging scenarios of FIGS. 5, 6 and 7, the server 24 is the message broker. The incoming and outgoing messaging types may differ or the same, as the message sending of each mobile system is linked using the database by the server.

It should be noted that field 332 data is similar to that as described in connection with element 302 of FIG. 5. In this instance however, the data included in the field 332 is mapped or translated to a format 334 to provide for the forwarding of SMS messages via existing Web SMS applications as per 42b of FIG. 1A.

What will now be described are generally how fields indicated in 332 are mapped or translated into those indicated in 334. The recipient's country 336c as previously described may be a country code selected from a pull-down list that may be displayed from a pull-down menu on a graphical user interface from a web page. The recipient's MIN or phone number 338b may be used in performing a query or search of the database to return the appropriate mobile network operator and return a URL for the Web SMS

22

location. For example, a URL may be returned indicating the address of a particular HTML page that indicates or hosts the particular application.

This application may be connected to the mobile network operators SMSC and forwards messages to users on that particular operators network. For example, the IP address or URL returns the messaging application web site of operator "x". The application on that site may require that the recipient's MIN number is entered, along with the message. A "send" button may then be used to submit the message. The operator's background application takes this message, and transforms it to an SMS message that may be processed by the operator's SMSC. From thereon, the message is forwarded to the recipient's handset as a conventional SMS. The Tiixa process emulates this process from the central server 24, in this way, forwarding the message on from the sender.

As a further example, the phone number "3057211234" may correspond to a mobile network operator or carrier having a corresponding URL, or an IP address. Part of the processing as previously described is transforming the recipient's MIN or phone number 338 into the particular mobile network operator's format, for example, using padding or stripping leading zeros or the portions of the numbers as needed. Many network operators having web based messaging systems use local short form numbering as the users are generally local. In this case, international form numbers have the country code removed. For example, a user may input a MIN format that may be 10 or 11 digits long. The routing database may indicate for a particular mobile network operator or carrier, only the last seven digits of the MIN may be used when sending a message to a user associated with that particular mobile network operator. Therefore the number representative of the recipient's phone number 338b when remapped or placed in a format 342 may include only the last seven digits of the MIN. The MIN in the fields described herein may be posted via HTTP to the fields or commands on the mobile network operator's existing web based SMS application.

Similarly as described in connection with the processing of the translation or mapping of FIG. 5, corresponding portions of the field are mapped or translated from 332 to that of 334. Additional optional processing may be performed for example to eliminate offensive text as also previously described. Once the message is placed in the format 334, the message may be sent and is received by the mobile network operator's web SMS application, translated, and passed via the SMSC to the recipients of the message. In other words, the web posting application mapping technique represented in illustration 330 described in connection with FIG. 6 may be used when a recipient's message is in a digital mobile network that uses a Web SMS application to translate messages received.

FIG. 1 takes the user perspective of "all connected" messaging. Note that as described elsewhere herein with all three messaging scenarios, the server 24 is the message broker. The incoming and outgoing messaging types could be different or the same, they are independent of one another, and logically linked only via the database. FIG. 1A shows the possible "output" forms, that is, from server 24 out to the recipient.

Referring now to FIG. 7, shown is a representation 360 of mapping input field 362 to a format 364 used in connection with a direct connection to an SMSC. It should generally be noted that the fields of 362 of FIG. 7 are similar to those described in connection with field 302 of FIG. 5 and 332 of FIG. 6. In other words, these fields may be input, for

## US 7,209,950 B2

23

example, using a form-like interface such in connection with a Web page, or alternatively received as a MO SMS as in connecting with user **16** of FIG. **1**. The incoming and outgoing messaging types may be different or the same, as they are independent of one another, and logically linked via the database and server at the “hub” of FIG. **1**.

Subsequently, these data fields input may be mapped to the format **364** in accordance with a particular format as indicated by the country code, MIN, and particular cellular carrier or operator with information as recorded in the routing database to produce the format **364**.

The recipient’s country code may be preselected such as included in field **366c**, for example, such as in connection with a pull-down user interface menu. A country-wide format form may accordingly be displayed in field **368a** (output field) as a template to serve as an example for entering the recipient’s phone number or MIN number **368b** (input field in accordance with **368a** format). Additionally, the message text or content may be entered in field **368c**. This is similar to other descriptions included elsewhere herein in connection with other figures.

Also as previously described, the routing database may be queried in accordance with the recipient’s MIN or phone number as indicated in field **368b**. Accordingly, routing information may be returned from the database in accordance with this particular MIN for particular countries selected. In this example, the forwarding method returned from the database may indicate integrated third-party application software. For example, the MIN or phone number “6912371234” may select cellular operation or carrier “Z” as a carrier and return an instruction to call the SMSC direct forwarding application.

The direct forwarding application may use as an input a unique configuration file for each different mobile network operator in which the specifications may vary in accordance with each cellular carrier or mobile network operator. In other words, a configuration or specification file **374** may be created with certain information as indicated in this particular example that may vary with each cellular carrier, operator and/or network. In this example, specifications included in the configuration file **374** may include the IP address of the SMSC of the recipient (127.1.1.1), the user name assigned by a mobile network operator for the connection on SMSC, a password, a protocol type of SMSC for example such as SMPP, a message type, and a message link. Similarly as described in connection with other figures the recipient’s phone number or MIN may be transformed from the country-wide MIN format into a mobile network operator-dependent format that may include, for example, truncating or padding digits as needed.

In this example, cellular operation “Z” may use the standard 10-digit MIN resulting in no change to the MIN in the output formatted message. Thus, the number as indicated in field **368b** may be copied directly to field **372a** without alterations. Other fields may also be copied and mapped as indicated in **360** FIG. **7**. The message in turn may be received by the mobile network operator and forwarded accordingly to the recipient. As the connection is direct to the SMSC, the message is not converted on reception by the SMSC. Rather, it may be forwarded directly to the recipient’s handset. Advantages exist in this type of connection, for example, in that it is known if the message is received successfully on the handset. The whole process is logged step by step, and these logs in turn may be filtered and modified to form billing information.

Referring now to FIG. **8**, shown is an example of a representation of one embodiment of a routing database that

24

may be used in connection with the processing for the routing database **22** described herein. The schema **400** includes tables representing data that may be included in one embodiment of the routing database as well as relationships between those tables. However, it should not be construed as a limitation as other embodiments may include additional information as well as additional types of mapping and relationships.

The representation **400** includes a stuffing table **402**, a Celcos table **404**, a numbers table **406**, a Message Type (Msg\_jtype) table **408**, and a Country\_Specs table **410**. In one embodiment, each of these tables may represent of format of information of a record.

For example, a record may exist in the routing database for each mobile network operator and include the information specified within the table **404** as fields of the record associated. Information may be stored in accordance with each particular “Celco” or mobile network operator such as AT&T, Verizon, Voice Stream, and the like. A unique ID or CelcosID **404a** may be stored for each mobile network operator as well as the name of Celco in field **404b**. An e-mail address may be included in field **404c** that follows the “@” sign when forming an e-mail address, or is indicated as “unknown” for incompatible celcos. Some network operators do not have messaging services available on their networks, for example, those operators using analogue mobile phones of the AMPS standard. These operators do however have MIN listings, and the system, server **24** and database **22**, understand that although a MIN exists, it does not automatically imply the MIN, and therefore the associated mobile device, may necessarily receive an SMS message.

The celco e-mail field **404c** may include, for example, the information included in field **314b** as previously described in connection with FIG. **5**. This may generally be thought of as the operators email extension. The Stuff code\_404d and the message code **404e** are fields in one embodiment that include information about the exact formatting of the message required for the returned mobile network operator. The Country field **406f** relates the mobile network operator to a geographical location or country. This may be later used to provide operator and language specific help to the users. The help feature is described elsewhere herein in more detail.

The Connection field **404g** describes the connectivity method used to connect from the central server **24**, to the cellular operator. The different method of connections, as described elsewhere herein, may include:

1. Direct connection via SMPP, UCP, OIS or similar
2. Email connection to the operators email gateway
3. Posting application to the operators Web SMS gateway

For example, the Motorola SMSC manufacturer as described elsewhere herein may support any one of three different types of protocols such as SMPP, SMTP for e-mail, and HTTP. The medium for transport may be one of, for example, modem, ISDM, X.25, X.31 or TCPIP. Information as to which protocol and transport medium as well as the particular SMSC manufacturer used by a particular celco is indicated elsewhere herein.

The Number\_chars field **404h** is used to return the maximum SMS message length supported by the destination mobile network operator. This is typically in the range of 90 to 160 characters, with some as long as 500 characters. Information given here is used by the process logic to determine if it is necessary to split and send as a series of concatenated SMS messages, or indeed to join split messages into one SMS message. For example, in the scenario shown in FIG. **1**, if user **16** has a messaging length **404h** of



## US 7,209,950 B2

25

160 characters, but the recipient **20** has 120 character messages, the message may be broken down and divided in the server **24** into multiple messages such as two messages, of the format 1 of 2 and 2 of 2. These multiple messages may be sent to ensure arrival in the correct sequential order.

The URL field in **404i** holds the URL or web link of the mobile network operator **404b**. This link can be used to point the user to the correct source for local help, for example, to request that the operator enables SMS or other messaging privileges. This information may be displayed in a variety of circumstances, for example, on detecting an error in the forwarding of a message. An example of the table **404** formats may be seen in FIG. 9.

The country specs table **410** may describe information regarding the country-wide MIN format, for example, used as a template in entering the recipient's phone number **308b**. From a user point of view, a single numbering convention may be preferred and shown for all mobile network operators in that country. This may avoid user confusion. The country specs table **410** in this example includes: a country **410a** which may be indicated as an alphanumeric or other type of abbreviation for each country, a code **410b** which may correspond to a country code from a pull-down list, digits **410c** indicating the number of digits that may occur in a phone number in the country-wide MIN format (this may be used as a checksum to compare quickly to the user input number, (e.g. Is the number the correct length?), an example phone number **410d** which may be displayed, for example, in field **308a**, and any additional comments **410e, f** and **g** that may be displayed in accordance with this particular field. The comments are in the appropriate language for the user, if the user is unknown the default is the country's language. A comment field **410h** allows any other pertinent information to be entered. An example of table **410** format can be seen in FIG. 10.

The message type table **408** is used to format the outgoing (from server **24**) message. As most messaging scenarios are basically the same, with small variations some message types can therefore be re-used on many different mobile network operators. The TypeID **408a** assigns a number to each of the used formats. The field TypeDesc **408b** describes in detail the type of message formatting operations performed by the application. Here are some examples of **408b**:

Put [Message] In The Email Subject—in this case the text enclosed as the message body is formatted to enter the subject field of the target mobile network operators SMS application.

Put [StuffedNumber [Message]] in Email Subject—in this case the Stuffed number (see **402** later) is placed alongside the message body within the email subject field.

A comment field **408c** allows any other pertinent information to be entered.

Further examples of table **408** can be seen in FIG. 11.

The Numbers Table **406** indicates that MIN or phone number ranges for each particular celco Id. This table is critical as it performs the initial lookup of the target mobile network operator, taking as its input an unknown MIN. The celco ID **406a** is that particular field for example identified in field **404a** used as a reference to index into the numbers Table **406**, this field is a short alphanumeric label that uniquely identifies all operators. The international country code **406b** is included, and is used in cases where the incoming MIN number has had the country code isolated from the rest of the number, this permits faster lookup as only the number in that country are scanned. See step **220** in FIG. 4 for an example of its use. An area code or cellular number prefix is included in the field **406c**, some countries

26

assign a unique code or access number to indicate that the recipient is a mobile device, others use normal area codes as for traditional telephony. Fields **406d** and **406e** identify ranges of phone numbers allocated by each particular operator. These numbers are the local form only, as they are without country code and prefix. This form may be used in some messaging systems using only local form MIN. Similarly, the fields **406f** and **406g** identify MIN or phone number allocation ranges that include the prefix identified in field **406c** and country code as in field **406b**. These number ranges are those generally consulted in the mobile network operator lookup process. As the numbers are in complete international form, they can may only one unique device associated worldwide, guaranteeing that the mobile network operator returned is the correct one. Record ID field **406h** is a unique identifier for each line of the database, this is needed for correct database operation and processing.

As an example of usage, if the sender **16** of FIG. 1 wishes to send a message or application to the recipient **20**, the following lookup occurs:

The sender **20** sends a message to the recipient **16**, the sender specifies the recipients MIN as 5693183098, types his message and sends it to the server **24**. At the server **24** the sender **20** is first authorized by comparing his MIN to the user database, if he is registered the recipients **20** number is looked up or scanned for in the ranges **406f** to **406g**. If the number is found, the corresponding mobile network operator is returned using the CelcoID **406a**. The sender's message is then processed in the server **24** according to the rules in the database for the returned celco ID **406a**, in particular regarding to formatting and sending method. Once reformatted, the message is sent out to recipient **20**.

Further examples of table **406** can be seen in FIG. 12.

The stuffing table **402** is used to format the outgoing (from server **24**) message. As most messaging scenarios are basically the same, with small variations some message types can therefore be re-used on many different mobile network operators. The Format **402a** assigns a number to each of the used formats and is basically a list pointer. The field Stuff code **402b** describes in detail the of required MIN formatting operations performed by the application. Here are some examples or **402b**:

(stuffed "0")(prefix)(stuffed "15")(number)@email—here the user input recipient MIN has a number 0 added, has the prefix **406c** added, has the number 15 added and then ends with the local form number. For example, if the sender **12** were to send a message to an recipient **20**, who corresponded to mobile network operator with this Stuff code, the input number may be: 234422 and the output number, after being modified in the server **24** application would be 05515234422. This would therefore be forwarded in this form to the recipient **20** mobile operators network.

A comment field **402c** allows any other pertinent information to be entered.

An example of the contents of table **402** can be seen in FIG. 13.

Here is an example of use of all the previously described fields in the routing database **24**:

A user may send a message to the number 5733321588. He prepares the message with the recipient's number located in either the message body, or in the "to" field of the MO SMS device and "sends" the message that is received on the mobile network operator's SMSC and then forwarded to the server **24**. The incoming message is parsed and authenticated and the routing database is consulted for the recipient's number, specifically in the ranges **406f** and **406g**. In this case, the number range is found to be associated to a

US 7,209,950 B2

27

Colombian operator called "operator B". In FIG. 8, sector 406a, "operator B's unique ID is then returned. The ID 406a associates the information in tables 404, and it's dependants 402 and 408. The ID returns the rules for formatting and processing the message. For example 404d points to lookup table 402.

In table 408 the message format type 408a is found, the message formatted accordingly in the correct fields. For example: the name of the sender is placed in the subject field of the outgoing message. In one example, "operator B" is accepted and, therefore the message is left in the message body.

The stuff code, 402b, adds or removes digits from the MIN to suit the operators numbering convention; some use international formats (like GSM operators, a typical number being +5693183098), and some use local format numbers (typical in TDMA operators, a typical number being 3183098). For example, when sending a message to a TDMA operator's SMSC, if the incoming number is in international format, the international country code may be removed before sending to the SMSC. If it is not removed, the SMSC may not recognize the recipient and not deliver the message, or think that there is an error. In this example, the "operator B" is TDMA, but the ID reveals the operator to be TDMA. The stuff code, 402b, indicates that the first two digits are removed. The number 5733321588 then becomes 33321588.

At this point, the message is formatted. It is determined How to send the message to "operator B". The ID relates to table 404, and field 404g is checked. In this case "SMPP app 2" is found forcing a DIRECT connection with the operator's SMSC. That loads the correct configuration file to the server 24. Fields and parameters are combined to form the message output. Finally, a check to determine if the incoming message is of the correct length to fit in to one outgoing message is performed with the information returned from 404h, number of character field. As the message is short in this example, it fits easily into one outgoing message.

To complete the above example, if the message to be sent is "how are you", the following may be spooled to the SMTP application for forwarding to the target mobile network operator:

Sending application name—operator B—33321588—how are you

The application starts, calling those details required for operator B, such as IP address, user name and password, and once connected to the remote SMSC, will submit the message as shown.

Additionally, techniques described herein may be used in facilitating communication via SMS between source and destination devices each using different underlying technology. For example, one cellular telephone may be a micro browser telephone using software providing for WWW connections and functionality associated therewith. This type of device may communicate, for example, with older devices.

The foregoing also provides a simplified mobile operator network number input format with examples, each of which is unique for country, in an effort to reduce user input error via the simplified format. The foregoing also includes a database having flexible construction to permit incorporation, for example, of new mobile network operators, and updating information and message delivery methods as needed. The foregoing techniques are included in a flexible system that may be used for any one of variety of different types of devices, for example, including micro browser cellular phones, or other types of devices, for example, that

28

may be included in a digital mobile network. The mobile device, for example, may include messaging capability. The foregoing techniques may be used to provide for the inter-connection of devices which are new as well as legacy older technologically based communication devices. Additionally, these devices for source and point of destination may be included in independent mobile operator networks, for example, each in accordance with their own standards and protocols. The user who is sending and receiving the messages has the advantage of having the processor forwarding a message in a streamline fashion using the foregoing techniques. The foregoing techniques may apply to a sender sending a message to one or more recipients.

The foregoing techniques consult a database to obtain information in accordance with a specified message recipient. The information may include, for example, country wide MIN format, an inquiry as to whether the database includes information corresponding to the particular recipient, and routing information associated with the digital mobile network of the particular recipient. Routing information may include, for example, message body format information and electronic mailing addressing format information. Checks may also be made to verify the length of the message sent and to be forwarded. Logging of all steps provides the framework to a billing and operator consolidation platform.

The foregoing techniques may also be used in sending electronic messages using a server between users in different digital mobile networks or pulling content using host or remote servers. A user may obtain information, such as, for example, weather and stock information, by "pulling" the information using the server. The user may communicate directly with the server to obtain the information requested. Alternatively, a user may communicate to the user's host SMSC. The server may then poll the host SMSC to receive the user's request for information. Also, applications, such as those requiring server processing of the received requests, may be sent back to the requesting party, or sent on to third parties. An example of such application is a Ringtone, a short musical theme used as the ringer on mobile devices. Such a ringtone may be requested by sending a message with the tones name or catalogue number to the central server. The central server then processes the request and returns the specially coded ringtone to the mobile device.

It should be noted that in the foregoing, a front end interface may be included in an embodiment, for example, using standard Internet protocols, allowing a user to enter and send messages using web-pages in accordance with configurations associated with, for example, FIGS. 1 and 1A. These web pages may be "served" to a user by the server 24.

Referring now to FIG. 9, shown is a more detailed example of stuffing table 402 of FIG. 8.

Referring now to FIG. 10, shown is a more detailed example of a Celcos table 404 of FIG. 8.

Referring now to FIG. 11, shown is a more detailed example of the Numbers table 406 of FIG. 8.

Referring now to FIG. 12, shown is a more detailed example of the Msg\_type table 408 of FIG. 8. It should be noted that FIG. 12 includes an additional field in this example, the application destination field 408d which, in this example, may be used as an extension to the comments field for informational purposes.

Referring now to FIG. 13, shown is a more detailed description of the Country\_specs table 410 of FIG. 8.

While the invention has been disclosed in connection with preferred embodiments shown and described in detail, their

## US 7,209,950 B2

29

modifications and improvements thereon will become readily apparent to those skilled in the art. Accordingly, the spirit and scope of the present invention should be limited only by the following claims.

What is claimed is:

1. A method executed in a computer system for routing a message from a sender in a first digital mobile network employing a first digital mobile network protocol to an intended receiver in a second different digital mobile network, the second digital mobile network employing a second digital mobile network protocol that is different from the first network protocol, the message comprising a message body and associated message routing information, the method comprising:

forwarding said message to a server from said sender, said server being connectable to said first and said second digital mobile network;

relating, using a routing database, a receiver identifier, the receiver identifier being contained in the associated message routing information and associated with the intended receiver, to corresponding routing format information associated with the second digital mobile network protocol, the routing format information associated with the second digital mobile network protocol comprising at least a second protocol mobile carrier interface format type and a second protocol mobile carrier addressing format type;

reformatting said associated message routing information into a format specified by said corresponding routing format information, wherein the reformatting is transparent to a sender and receiver of the message and the message body remains unchanged, by the steps of: translating the receiver identifier to a destination address that conforms to the second protocol mobile carrier addressing format type;

placing the destination address into a reformatted message that has a structure that conforms to the second protocol mobile carrier interface format type; and placing the message body unchanged into the reformatted message in a manner that conforms to the second protocol mobile carrier interface format type; and

forwarding said reformatted message to said receiver in accordance with the reformatted associated message routing information.

2. The method of claim 1, wherein said message is a short message service message.

3. The method of claim 1, wherein the sender sends the message and the receiver receives the message using at least one of:

digital mobile device connected to the internet, digital mobile device connected to the server through a service center of an associated mobile network operator, and computer system connected to the internet.

4. The method of claim 1, further comprising: performing a first query using the routing database to determine a countrywide mobile identification number format of a country associated with the receiver.

5. The method of claim 4, further comprising: performing a second query using the routing database to determine if information identifying the receiver is included in the routing database.

6. The method of claim 5, further comprising: performing a third query using the routing database to determine said routing information associated with the second digital mobile network of the receiver, said routing information including at least one of: format of a message, electronic mail address format, and message delivery method.

30

7. The method of claim 6, wherein routing information including a message delivery method uses one of: a direct connection to an operator, an application, and e-mail connection.

8. The method of claim 1, further comprising: polling said server by the sender for data.

9. The method of claim 8, further comprising: communicating a request for data to said server.

10. The method of claim 9, wherein said communicating a request for data to said server further comprises: directly sending a message to the server requesting information.

11. The method of claim 9, wherein said communicating a request for data to said server, further comprises: communicating the request for data to a messaging service center in said first digital mobile network; polling, by said server, the messaging service center for the request; and transmitting the request to said server.

12. The method of claim 11, wherein the request includes a keyword, said keyword being one of: a command and a phone number.

13. The method of claim 12, wherein the request is for at least one of:

stock information, weather information for a particular location identified in the message, and an application.

14. The method of claim 13, wherein a requested application is at least one of:

a game, ringtones in connection with audio tones, and a chat service.

15. The method of claim 1, wherein said sender is sending the message to a plurality of users, each of said plurality of users receiving the message being on different digital mobile networks.

16. The method of claim 15, further comprising: determining which of said plurality of users receiving the message are included in a buddy list, said buddy list including user specific information for message recipients; and

reformatting said message in accordance with a format associated with a particular digital mobile networks network for each of said plurality of users on different digital mobile networks.

17. The method of claim 16, further comprising: determining if a message recipient is within the first digital mobile network of said sender.

18. The method of claim 17, further comprising: reformatting an electronic mailing address from a first format associated with said first digital mobile network to a second format associated with the second digital mobile network.

19. The method of claim 1, wherein said computer system includes said server and a plurality of different digital mobile networks, said plurality of different digital mobile networks including said first and said second digital mobile networks, communications within said computer system being represented as a hub-like structure with said server as the center and each of said plurality of digital mobile networks being a spoke extending from said server, all communications between any two of said plurality of digital mobile networks being facilitated by said server.

20. The method of claim 19, wherein the message is sent between a sender and receiver independent of operator, location, and network protocols using said server.

21. A computer program product for routing a message from a sender in a first digital mobile network employing a first digital mobile network protocol to an intended receiver in a second different digital mobile network, the second digital mobile network employing a second digital mobile network protocol that is different from the first network



## US 7,209,950 B2

31

protocol, the message comprising a message body and associated message routing information, the method comprising:

machine executable code for forwarding said message to a server from said sender, said server being connectable to said first and said second digital mobile networks;

machine executable code for relating, using a routing database, a receiver identifier, the receiver identifier being contained in the associated message routing information and associated with the intended receiver to corresponding routing format information associated with the second digital mobile network protocol, the routing format information associated with the second digital mobile network protocol comprising at least a second protocol mobile carrier interface format type and a second protocol mobile carrier addressing format type;

machine executable code for reformatting said associated message routing information into a format specified by said corresponding routing format information, wherein the reformatting is transparent to a sender and receiver of the message and the message body remains unchanged, by the steps of:

translating the receiver identifier to a destination address that conforms to the second protocol mobile carrier addressing format type;

placing the destination address into a reformatted message that has a structure that conforms to the second protocol mobile carrier interface format type; and

placing the message body unchanged into the reformatted message in a manner that conforms to the second protocol mobile carrier interface format type; and

machine executable code for forwarding said reformatted message to said receiver in accordance with the reformatted associated message routing information.

22. The computer program product of claim 21, wherein said message is a short message service message.

23. The computer program product of claim 21, wherein the sender sends the message and the receiver receives the message using at least one of:

digital mobile device connected to the internet, digital mobile device connected to the server through a service center of an associated mobile network operator, and computer system connected to the internet.

24. The computer program product of claim 21, further comprising:

machine executable code for performing a first query using the routing database to determine a countrywide mobile identification number format of a country associated with the receiver.

25. The computer program product of claim 24, further comprising:

machine executable code for performing a second query using the routing database to determine if information identifying the receiver is included in the routing database.

26. The computer program product of claim 25, further comprising:

machine executable code for performing a third query using the routing database to determine said routing information associated with the second digital mobile network of the receiver, said routing information including at least one of:

format of a message, electronic mail address format, and message delivery method.

32

27. The computer program product of claim 21, further comprising:  
machine executable code for polling, by the sender, said server for data.

28. The computer program product of claim 27, further comprising:

machine executable code for communicating a request for data to said server.

29. The computer program product of claim 28, wherein said machine executable code for communicating a request for data to said server further comprises:

machine executable code for directly sending a message to the server requesting information.

30. The computer program product of claim 28, wherein said machine executable code for communicating a request for data to said server, further comprises machine executable code for:

communicating the request for data to a messaging service center in said first digital mobile network;

polling, by said server, the messaging service center for the request; and

transmitting the request to said server.

31. The computer program product of claim 30, wherein the request includes a keyword, said keyword being one of: a command and a phone number.

32. The computer program product of claim 30, wherein the request is for one of:

stock information and weather information for a particular location identified in the message.

33. The computer program product of claim 21, wherein said sender is sending the message to a plurality of users, each of said plurality of users receiving the message being on different digital mobile networks.

34. The computer program product of claim 33, further comprising:

machine executable code for determining which of said plurality of users receiving the message are included in a buddy list, said buddy list including user specific information for message recipients; and

machine executable code for reformatting said message in accordance with a format associated with a particular digital mobile network for each of said plurality of users on different digital mobile networks.

35. The computer program product of claim 34, further comprising:

machine executable code for determining if a message recipient is within the first digital mobile network of said sender.

36. The computer program product of claim 35, further comprising:

machine executable code for reformatting an electronic mailing address from a first format associated with said first digital mobile network to a second format associated with the second digital mobile network.

37. The computer program product of claim 21, wherein said computer system includes said server and a plurality of different digital mobile networks, said plurality of different digital mobile networks including said first and said second digital mobile networks, communications within said computer system being represented as a hub-like structure with said server as the center and each of said plurality of digital mobile networks being a spoke extending from said server, all communications between any two of said plurality of digital mobile networks being facilitated by said server.

38. The computer program product of claim 37, wherein the message is sent between a sender and receiver independent of operator, location, and network protocols using said server.



UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,209,950 B2  
APPLICATION NO. : 09/921167  
DATED : April 24, 2007  
INVENTOR(S) : Simon Bennett et al.

Page 1 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 1, line 27, after “network operator network” insert -- of that --;  
line 34, delete “to” and insert -- with --.

Column 2, line 32, delete “FIG. 2 is” and insert -- FIGS. 2A and B depict --.  
line 36, delete “FIG. 3 is” and insert -- FIGS. 3A-C depict --.  
line 41, delete “FIG. 4 is” and insert -- FIGS. 4A and B depict --.

Column 10, line 5, delete “FIG. 2” and insert -- FIGS. 2A and 2B --;  
line 10, delete “FIG. 2” and insert -- FIGS. 2A and 2B --.  
line 44, delete “Fig. 2” and insert -- FIG. 2A --.

Column 11, line 12, delete “Fig. 2” and insert -- FIG. 2A --.

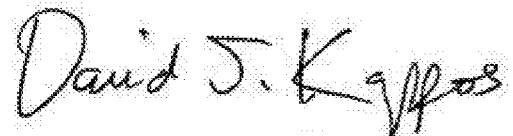
Column 12, line 29, delete “FIG. 2” and insert -- FIGS. 2A and 2B --.  
line 56, delete “FIG. 2” and insert -- FIGS. 2A and 2B --;  
line 61, delete “FIG. 2” and insert -- FIGS. 2A and 2B --;  
line 63, delete “FIG. 3” and insert -- FIGS. 3A-C --;  
line 67 and at column 13, line 1, delete “FIG. 3” and insert -- FIGS. 3A-C --.

Column 13, line 43, delete “FIG. 3” and insert -- FIG. 3A --;  
line 59, delete “FIG. 3” and insert -- FIG. 3A --.

Column 15, line 31, delete “FIG. 2” and insert -- FIGS. 2A and 2B --;  
line 36, delete “FIG. 2”, first occurrence and insert -- FIG. 2B --;  
lines 36 and 37, delete “FIG. 2” and insert -- FIGS. 2A and 2B --.  
line 56, delete “FIG. 4” and insert -- FIGS. 4A and 4B --.

Column 16, line 29, delete “FIG. 2” and insert -- FIGS. 2A and 2B --;  
line 34, delete “FIG. 2” and insert -- FIG. 2B --.

Signed and Sealed this  
Seventeenth Day of May, 2011

A handwritten signature in black ink, reading "David J. Kappos". The signature is written in a cursive, flowing style with a large initial 'D' and 'K'.

David J. Kappos  
*Director of the United States Patent and Trademark Office*

**CERTIFICATE OF CORRECTION (continued)**

Page 2 of 4

**U.S. Pat. No. 7,209,950 B2**

line 37, delete “FIG. 3” and insert -- FIGS. 3A-C --;  
line 42, delete “FIG. 2” and insert -- FIGS. 2A and 2B --.

Column 17, line 13, delete “FIG. 3” and insert -- FIGS. 3A-C --.  
line 52, delete “FIG. 3” and insert -- FIGS. 3A-C --.

Column 18, line 8, delete “FIG. 4” and insert -- FIGS. 4A and 4B --;  
line 13, “FIG. 4” and insert -- FIGS. 4A and 4B --.

Column 21, line 15, delete “the FIG. 300” and insert -- FIG. 5 --.

Column 23, line 56, delete “360” and after “FIG. 7” insert -- 360 --.

Column 25, line 66 delete “FIG. 4” and insert -- FIG. 4A --.

Column 29, line 6, cancel the text beginning with “1. A method executed” to and ending “routing information.” in column 29, line 44, and insert the following claim:

-- 1. A method executed in a computer system for routing a message from a sender in a first digital mobile network employing a first digital mobile network protocol to an intended receiver in a second different digital mobile network, the second digital mobile network employing a second digital mobile network protocol that is different from the first network protocol, the message comprising a message body and associated message routing information, the method comprising:

forwarding said message to a server from said sender, said server being connectable to said first and said second digital mobile network;

relating, at the application layer using a routing database, a receiver identifier, the receiver identifier being contained in the associated message routing information and associated with the intended receiver, to a method associated with a network connection type associated with the second digital mobile network and corresponding routing format information associated with the second digital mobile network protocol, the routing format information associated with the second digital mobile network protocol comprising at least a second protocol mobile carrier interface format type and a second protocol mobile carrier addressing format type;

reformatting said associated message routing information into a format specified by said corresponding routing format information, wherein the reformatting is transparent to a sender and receiver of the message and the message body remains unchanged, by the steps of:

translating the receiver identifier to a destination address that conforms to the second protocol mobile carrier addressing format type;

placing the destination address into a reformatted message that has a structure that conforms to the second protocol mobile carrier interface format type; and

placing the message body unchanged into the reformatted message in a manner that conforms to the second protocol mobile carrier interface format type; and

forwarding said reformatted message to said receiver in accordance with the method associated with the network connection type and the reformatted associated message routing information. --

**CERTIFICATE OF CORRECTION (continued)**  
**U.S. Pat. No. 7,209,950 B2**

Page 3 of 4

Column 29, line 57, cancel the text beginning with “5. The method of claim 4” to and ending “included in the routing database.” at line 60 and insert the following claim:

-- 5. The method of claim 1, the step of relating further comprising:  
performing a query using the routing database to determine a countrywide mobile  
identification number format of a country associated with the receiver. --

Column 29, line 61, cancel the text beginning with “6. The method of claim 5” to and ending “and message delivery method.” at line 67 and insert the following claim:

-- 6. The method of claim 1 the step of relating further comprising:  
performing a query using the routing database to determine if information related to the  
receiver is included in the routing database and returning an error message if the information is not  
found. --

Column 30, line 1, cancel the text beginning with “7. The method of claim 6” to and ending “e-mail connection.” at line 4 and insert the following claim:

-- 7. The method of claim 1, the step of relating further comprising:  
performing a query using the routing database to determine said routing information  
associated with the second digital mobile network of the receiver, said routing information including  
at least;  
an electronic mail address format. --

Column 30, line 5, cancel the text: “8. The method of claim 1, further comprising: polling said server  
by the sender for data.” and insert the following claim:

-- 8. The method of claim 1, wherein the method associated with the network connection type  
uses at least one of:  
a direct connection to an operator, an application, and an e-mail connection. --

Column 30, line 62, cancel the text beginning with: “21. A computer program product” to and ending  
“associated message routing information.” and insert the following claim:

-- 21. A computer program product stored on a computer storage media for routing a  
message from a sender in a first digital mobile network employing a first digital mobile network  
protocol to an intended receiver in a second different digital mobile network, the second digital mobile  
network employing a second digital mobile network protocol that is different from the first network  
protocol, the message comprising a message body and associated message routing information,  
comprising:

machine executable code for forwarding said message to a server from said sender, said server  
being connectable to said first and said second digital mobile networks;

machine executable code for relating, at the application layer using a routing database,  
a receiver identifier, the receiver identifier being contained in the associated message routing  
information and associated with the intended receiver to a method associated with a network

**CERTIFICATE OF CORRECTION (continued)**

Page 4 of 4

**U.S. Pat. No. 7,209,950 B2**

connection type associated with the second digital mobile network and corresponding routing format information associated with the second digital mobile network protocol, the routing format information associated with the second digital mobile network protocol comprising at least a second protocol mobile carrier interface format type and a second protocol mobile carrier addressing format type;

machine executable code for reformatting said associated message routing information into a format specified by said corresponding routing format information, wherein the reformatting is transparent to a sender and receiver of the message and the message body remains unchanged, translating the receiver identifier to a destination address that conforms to the second protocol mobile carrier addressing format type, placing the destination address into a reformatted message that has a structure that conforms to the second protocol mobile carrier interface format type, and placing the message body into the reformatted message in a manner that conforms to the second protocol mobile carrier interface format type; and

machine executable code for forwarding said reformatted message to said receiver in accordance with the method associated with the network connection type and the reformatted associated message routing information. --

Column 31, line 46, cancel the text beginning with “24. The computer program product of claim 21” to and ending “associated with the receiver.”, and insert the following claim:

-- 24. The computer program product of claim 21, further comprising:

machine executable code for performing a query using the routing database to determine a countrywide mobile identification number format of a country associated with the receiver. --

Column 31, line 52, cancel the text beginning with “25. The computer program product” to and ending “included in the routing database.”, and insert the following claim:

-- 25. The computer program product of claim 21, further comprising:

machine executable code for performing a query using the routing database to determine if information related to the receiver is included in the routing database and returning an error message if the information is not found. --

Column 31, line 58, cancel the text beginning with “26. The computer program product” to and ending “and message delivery method.”, and insert the following claim:

-- 26. The computer program product of claim 25, further comprising:

machine executable code for performing a query using the routing database to determine said routing information associated with the second digital mobile network of the receiver, said routing information including at least  
an electronic mail address format. --

# Exhibit O

---



US007937081B2

(12) **United States Patent**  
**Phan-Anh et al.**

(10) **Patent No.:** **US 7,937,081 B2**  
(45) **Date of Patent:** **May 3, 2011**

(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

(75) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Helsinki (FI); **Stefano Faccin**, Dallas, TX (US)

(73) Assignee: **Spyder Navigations L.L.C.**,  
Wilmington, DE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **12/720,862**

(22) Filed: **Mar. 10, 2010**

(65) **Prior Publication Data**  
US 2010/0167735 A1 Jul. 1, 2010

**Related U.S. Application Data**

(62) Division of application No. 09/802,861, filed on Mar. 12, 2001.

(51) **Int. Cl.**  
**H04W 24/00** (2009.01)

(52) **U.S. Cl.** ..... **455/424**; 455/435.1; 455/415;  
455/433; 370/328; 370/338

(58) **Field of Classification Search** ..... 455/424,  
455/435.1, 415, 433; 370/328, 338  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,077,830 A 12/1991 Mallia  
5,463,672 A 10/1995 Kage  
5,561,854 A 10/1996 Antic et al.

6,097,942 A 8/2000 Laiho  
6,163,532 A 12/2000 Taguchi et al.  
6,408,182 B1 6/2002 Davidson et al.  
6,411,632 B2 6/2002 Lindgren et al.  
6,445,911 B1 9/2002 Chow et al.  
6,587,882 B1 7/2003 Inoue et al.  
6,594,490 B1 7/2003 Toyoda et al.  
6,600,920 B1 7/2003 Stephens et al.  
6,636,491 B1 10/2003 Kari et al.  
6,654,606 B1 11/2003 Foti et al.  
6,707,813 B1 3/2004 Hasan et al.  
6,721,291 B1 4/2004 Bergenwall et al.  
6,732,177 B1 5/2004 Roy

(Continued)

**OTHER PUBLICATIONS**

International Preliminary Examination Report for PCT/IB02/00721 completed Apr. 3, 2003.  
International Search Report for PCT/IB02/00721, mailed Feb. 26, 2003.

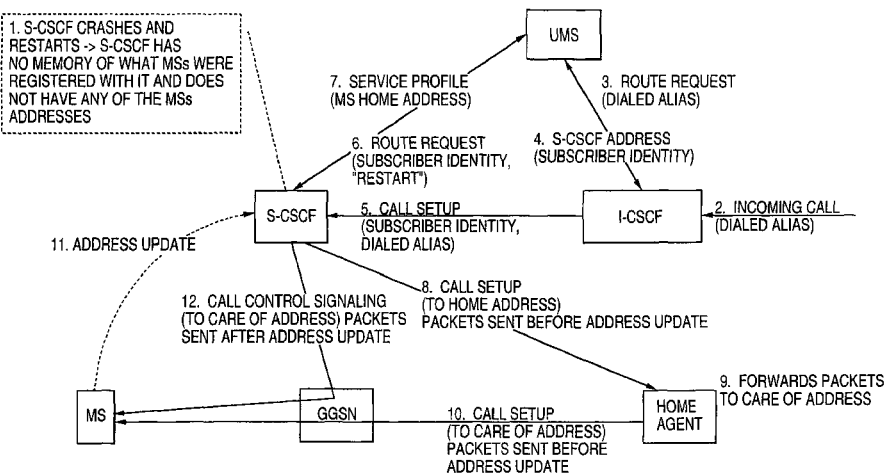
(Continued)

*Primary Examiner* — Nghi H Ly

(57) **ABSTRACT**

A technique for protecting location information of a subscriber in a mobile network is disclosed which forwards a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding a location update from the S-CSCF to an HSS including the subscriber's TA. Upon the S-CSCF losing data, lost data may be restored to the S-CSCF from the data stored in the HSS. The HSS may store data in a non-volatile memory such as a hard disk drive. The technique may also include forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding a location update from the S-CSCF to an HSS and storing data in a non-volatile memory such as a hard disk drive in the S-CSCF so as to be protected against loss. Upon the S-CSCF losing data, lost data including the subscriber's TA may be restored to the S-CSCF from the data stored in the S-CSCF.

**38 Claims, 6 Drawing Sheets**



**US 7,937,081 B2**

Page 2

---

U.S. PATENT DOCUMENTS

6,763,233 B2 7/2004 Bharatia  
6,775,255 B1 8/2004 Roy  
6,839,323 B1 1/2005 Foti  
7,602,762 B1 \* 10/2009 Kauppinen et al. .... 370/349

OTHER PUBLICATIONS

Technical Report TR 23.821 V1.0.1, published Jul. 2000 by the 3rd  
Generation partnership Project 3GPP.  
\* cited by examiner



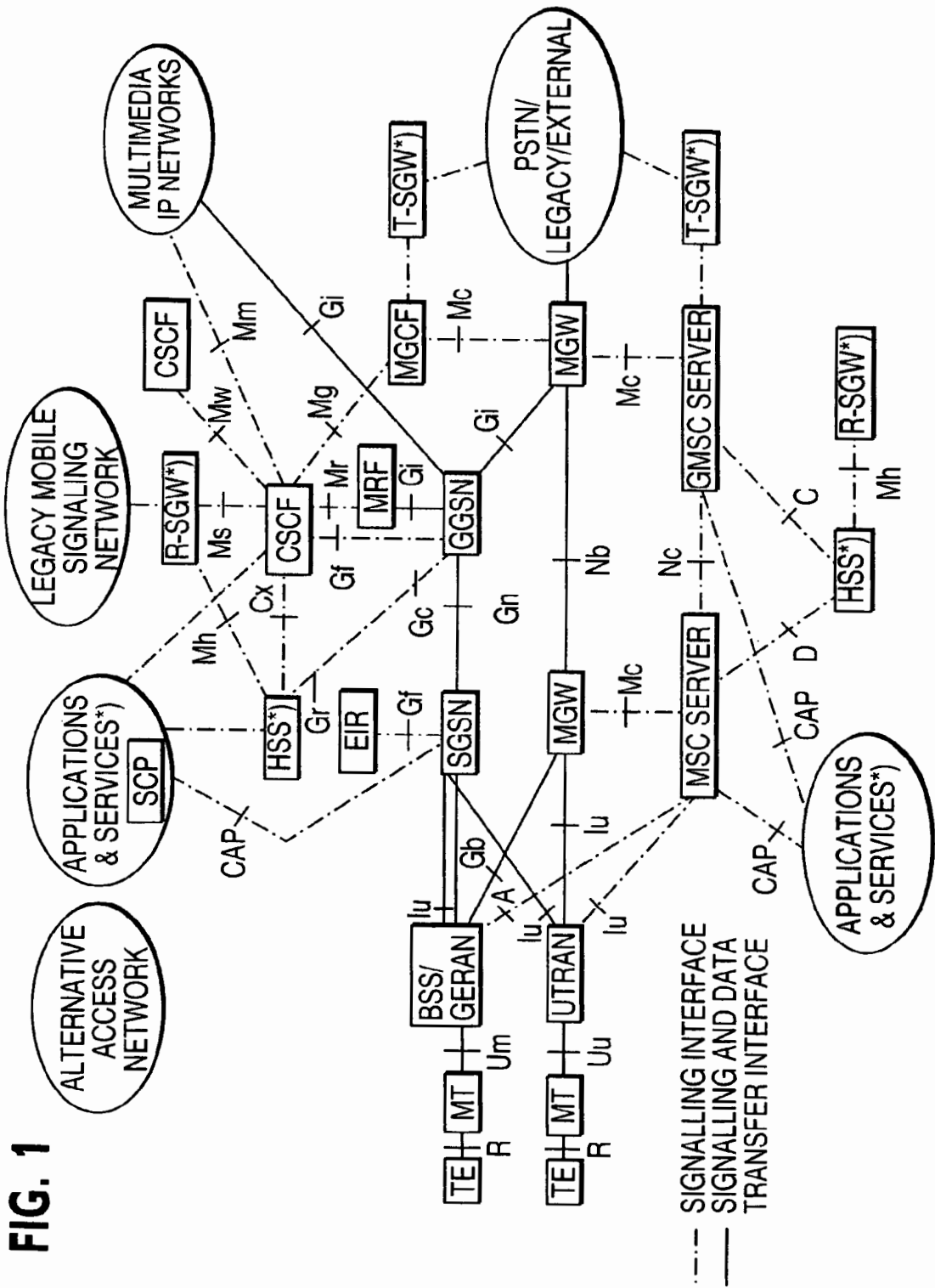


FIG. 2

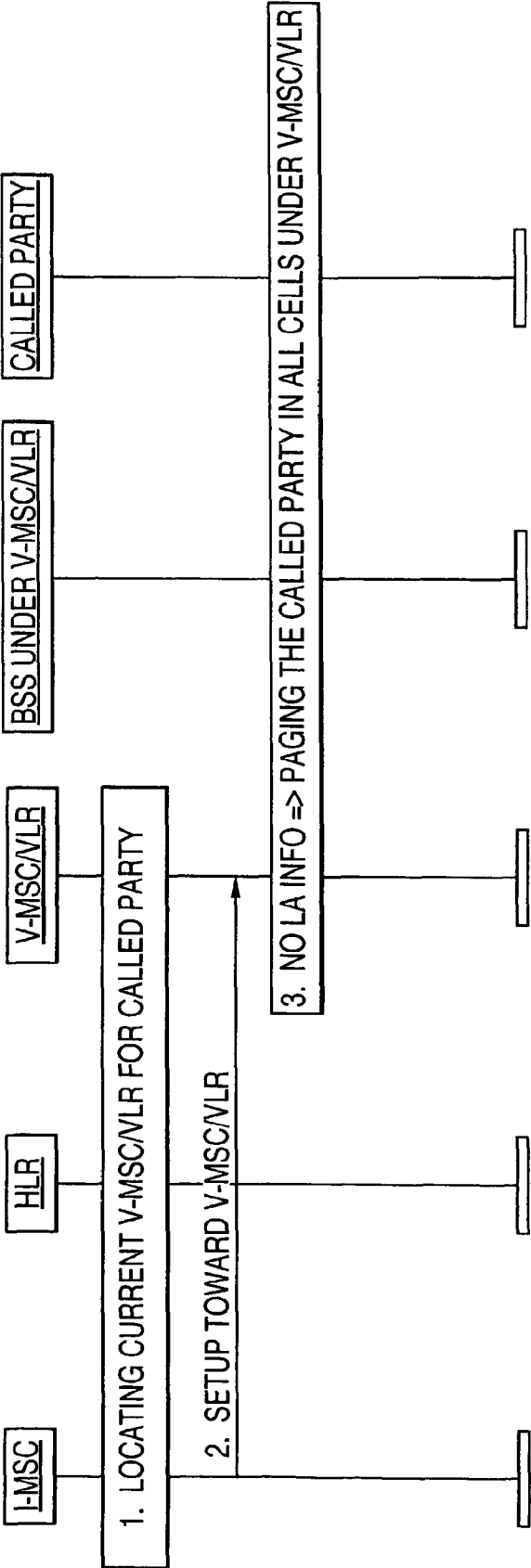
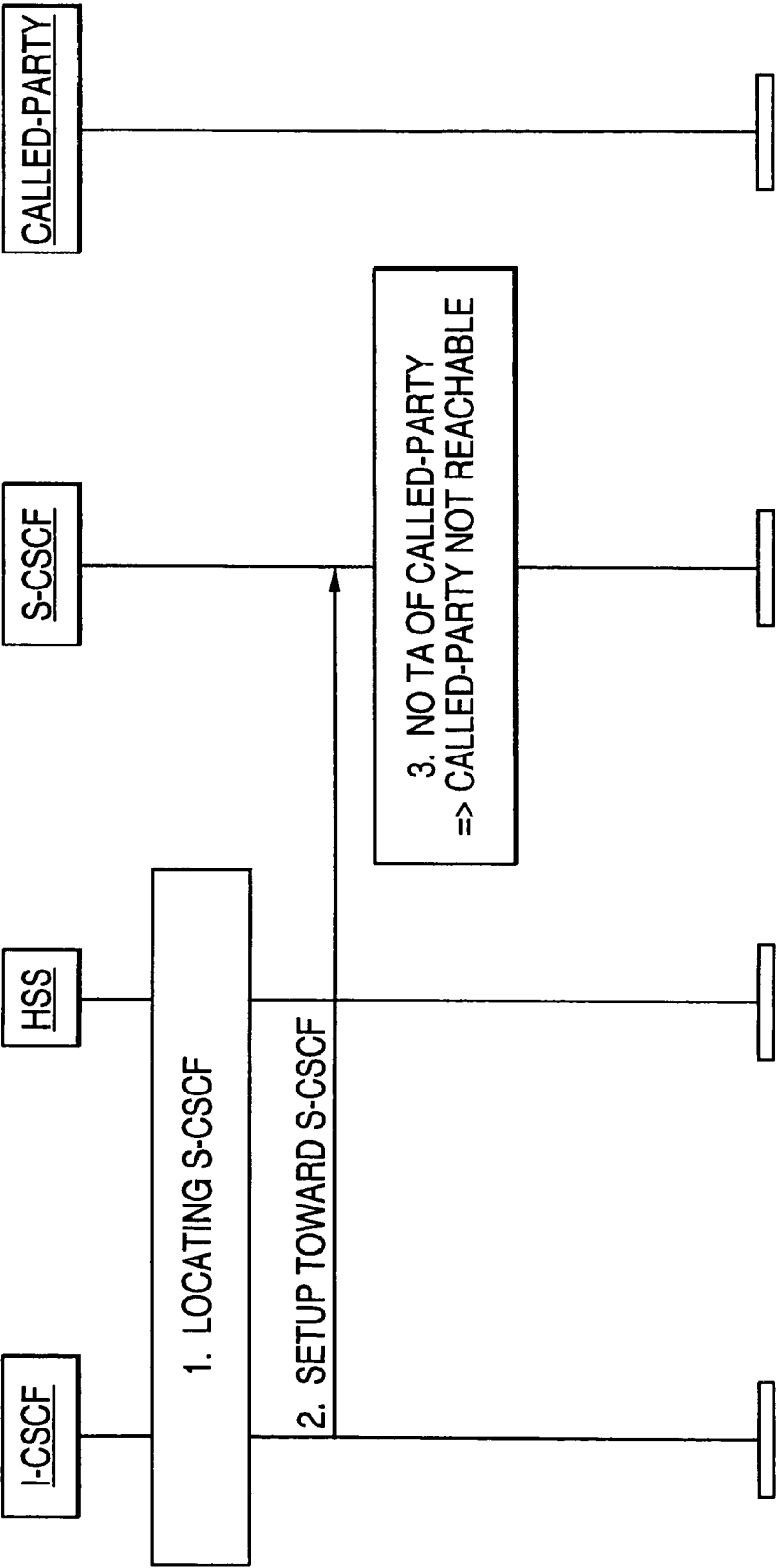


FIG. 3



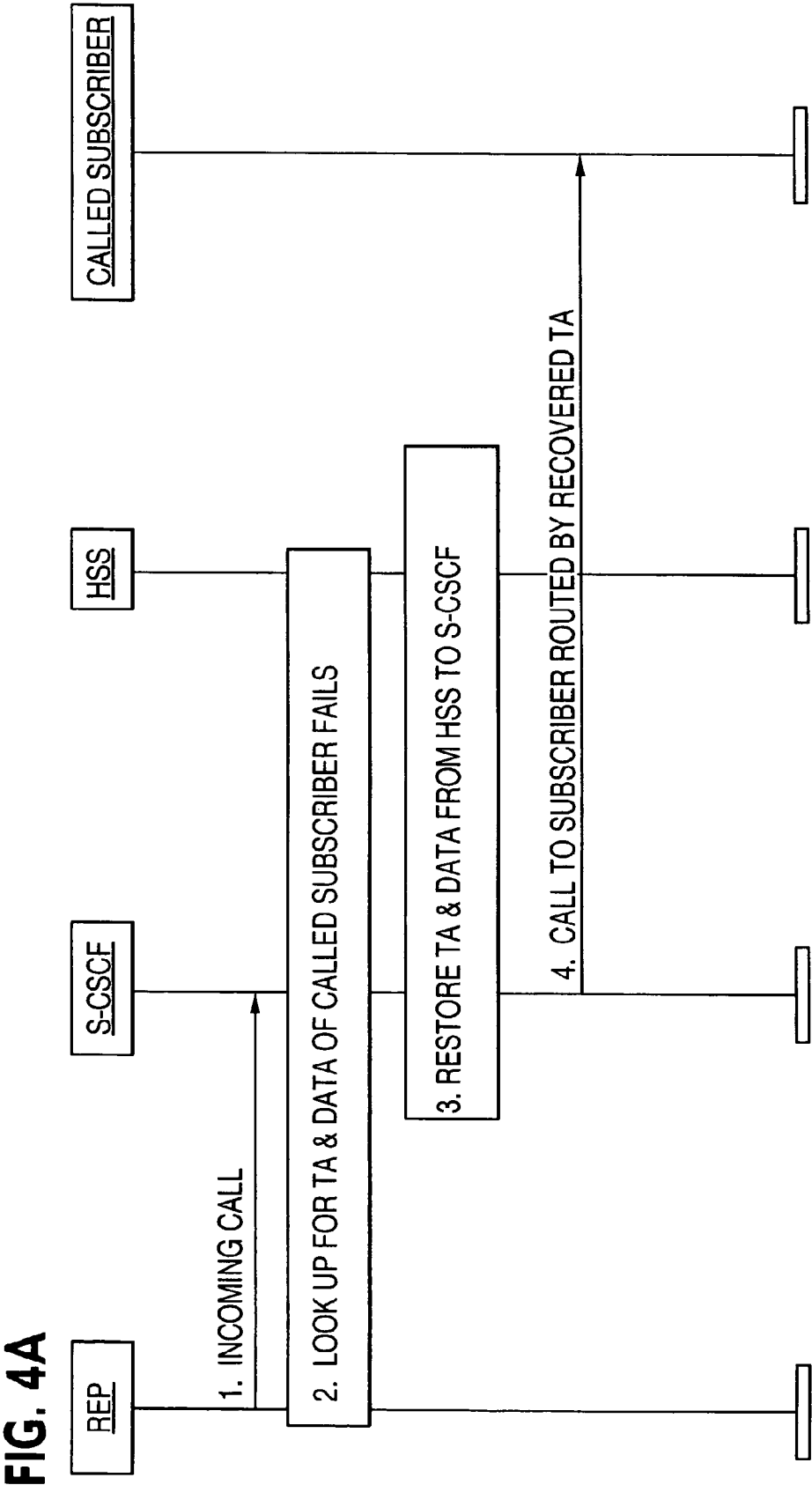


FIG. 4B

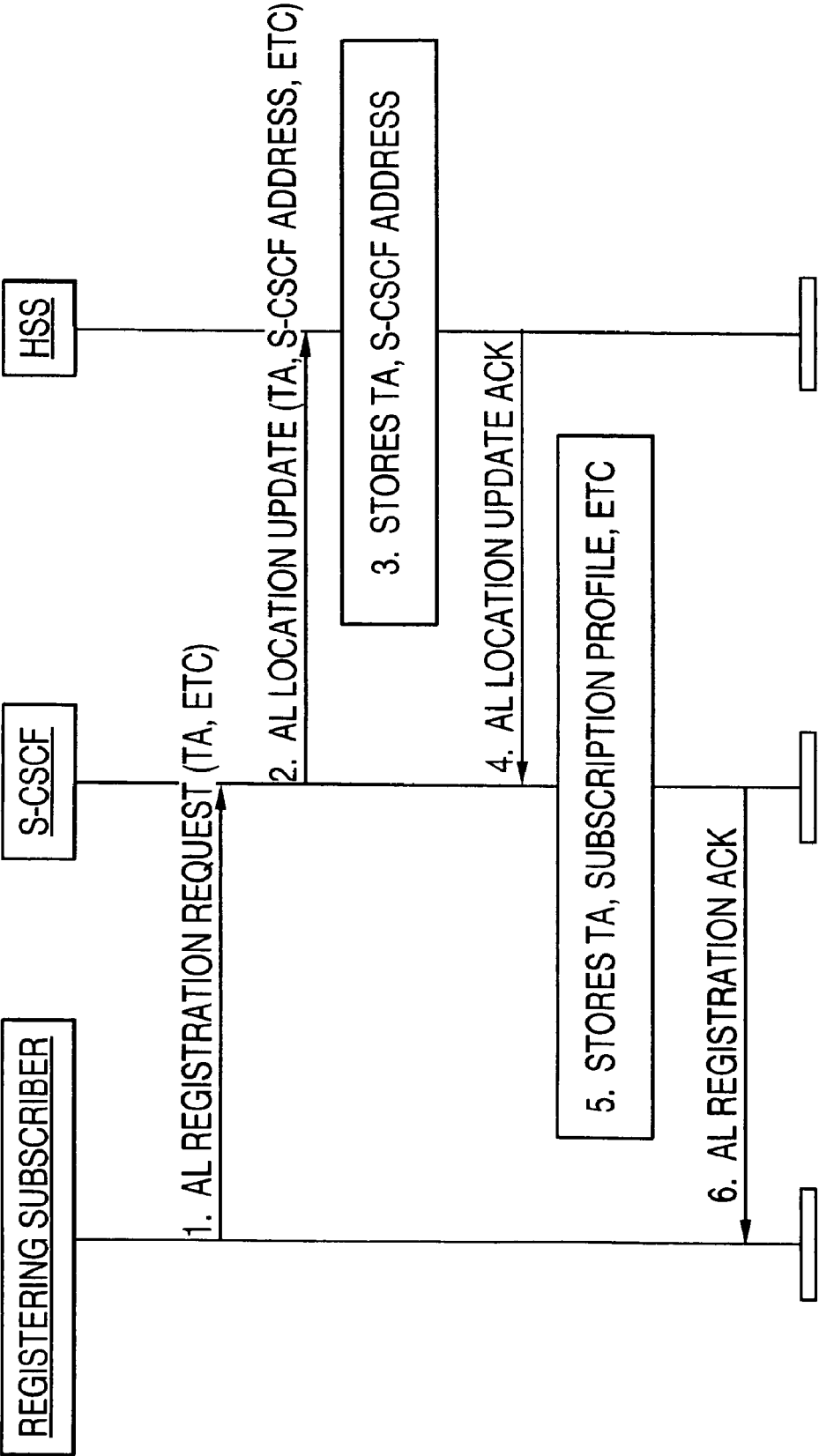
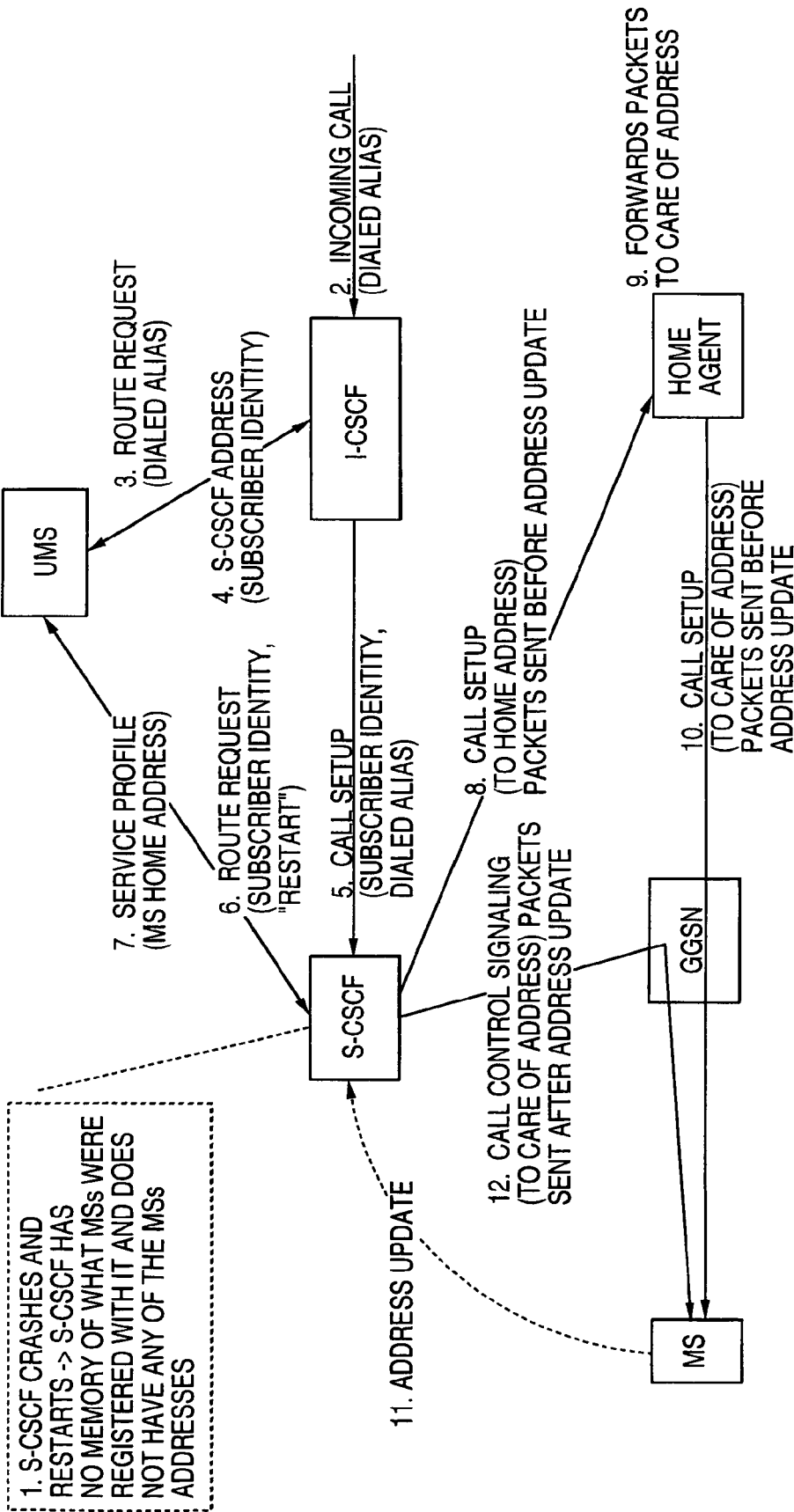


FIG. 5





US 7,937,081 B2

1

**RECOVERY TECHNIQUES IN MOBILE NETWORKS****CROSS-REFERENCE TO RELATED PATENT APPLICATIONS**

This application is a Division of U.S. patent application Ser. No. 09/802,861, filed Mar. 12, 2001, which is incorporated herein by reference in its entirety.

**FIELD**

The present disclosure relates to recovery techniques for use in mobile networks. More particularly, the present disclosure relates to protecting the Transport Address (TA) which is a current Care of Address of a mobile subscriber is reachable from loss and after Call State Control Function (CSCF) crashes and after reset situations of a network element realizing CSCF functionality.

**DESCRIPTION OF RELATED ART**

Technical Report TR 23.821 V1.0.1, published July 2000 by the 3rd Generation Partnership Project (3GPP) and available on the Internet at <http://www.3gpp.org>, discloses the specifications of a 3G All-IP mobile network and this report is incorporated by reference herein in its entirety.

FIG. 1 illustrates the architecture of the network disclosed in the above-noted Technical Report. The elements shown with asterisks are elements which have been duplicated for figure layout purposes only. These duplicated elements belong to the same logical element in the reference model.

Unfortunately, the network disclosed in the Technical Report fails to include any protection of the TA of a 3G All-IP subscriber from loss. Furthermore, the network disclosed in the Technical Report fails to protect the IP address of a subscriber in the case of a reset situation of a network element realizing CSCF functionality, that is, a CSCF, thereby preventing recovery after a reset of the network element. Still furthermore, the network disclosed in the Technical Report fails to protect the location information of a subscriber after a CSCF crash, thereby preventing recovery after a CSCF crash.

**SUMMARY**

An object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL (Application Level) location update from the S-CSCF to a Home Subscriber Server (HSS) including the subscriber's TA and the (S-CSCF) address and storing data including the subscriber's TA and the S-CSCF address in the HSS so as to be protected against loss.

Another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL location update from the S-CSCF to an HSS including the S-CSCF address and storing data including the subscriber's TA in a non-volatile memory of the S-CSCF so as to be protected against loss.

Yet another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including upon an S-CSCF receiving a call setup request for the subscriber from an Interrogating Call State Control Function (I-CSCF), forwarding a route

2

request to a User Mobility Server (UMS) and receiving a home address of the subscriber and then forwarding the call setup request from the S-CSCF to a home agent at the home address of the subscriber and then forwarding the call setup request from the home agent to the subscriber and subsequently forwarding an address update from the subscriber to the S-CSCF.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing and a better understanding of the present disclosure will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this disclosure. While the foregoing and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, issued a clearly understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 illustrates the architecture of a 3G All-IP mobile network.

FIG. 2 illustrates reaching a called party after losing LA (Location Area) information in a legacy mobile network.

FIG. 3 illustrates failure to reach a called party after losing TA information in a 3GPP All-IP mobile network.

FIG. 4A illustrates sending subscriber TA to S-CSCF and then forwarding it to HSS at registration.

FIG. 4B illustrates an example of reaching a called party after losing TA information in a mobile network in accordance with the present disclosure.

FIG. 5 illustrates the signal flow in the case of a recovery after a CSCF crash in accordance with another embodiment of the present disclosure.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Before beginning a detailed description of the subject disclosure, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, other components may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

In the application level of a 3G All-IP network, the reachability of a subscriber is maintained in two levels, namely, the network element level and the subscriber level. The S-CSCF that the subscriber is currently registered to and the TA of the roaming subscriber, which the subscriber provides to the network during Application Level (AL) registration, must be known to and maintained by the network.

Without specific support for mobility in IPv6, packets destined to a mobile subscriber would not be able to reach it while the subscriber is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a subscriber could change its IP address each time

US 7,937,081 B2

3

it moves to a new link, but it would then not be able to maintain transport and higher-layer connections when it changes location.

Mobile IPv6 allows a subscriber to move from one link to another without changing its IP address. A subscriber is always addressable by its “home address”, an IP address assigned to it within its home subnet prefix on its home link. Packets may be routed to the subscriber using this address regardless of its current point of attachment to the Internet, and it may continue to communicate with others after moving to a new link. The movement of a subscriber away from its home link is thus transparent to transport and higher-layer protocols and applications.

A mobile subscriber is always addressable by its home address, whether it is currently attached to its home link or is away from home. While it is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if it were never mobile. Since the subnet prefix of its home address is the subnet prefix (or one of the subnet prefixes) on the subscribers’ home link (it is the mobile subscribers’ home subnet prefix), packets addressed to it will be routed to its home link.

While a subscriber is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while the subscriber is visiting a particular foreign link. The subnet prefix of a subscriber’s care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by it; if it is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the subscriber in its location away from home.

The association between a subscriber’s home address and care-of address is known as a “binding” for the subscriber. It typically acquires its care-of address through stateless or stateful Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static preassignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this discussion.

While away from home, a mobile subscriber registers one of its care-of addresses with a router on its home link, requesting this router to function as the “home agent” for it. This binding registration is done by the subscriber sending to the home agent a packet containing a “Binding Update” destination option; the home agent then replies to the subscriber by returning a packet containing a “Binding Acknowledgment” destination option. The care-of address in this binding registered with its home agent is known as the subscriber’s “primary care-of address”. The subscribers’ home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the subscribers’ home address (or home addresses) on the home link and tunnels each intercepted packet to the subscribers’ primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation, with the outer IPv6 header addressed to the subscribers’ primary care-of address.

Keeping the address of the S-CSCF ensures that a call to a subscriber can be routed to the destination node, that is, the S-CSCF. Keeping the current TA of the subscriber ensures that a call made to the subscriber which arrives at the S-CSCF can finally reach the subscriber.

As illustrated in FIG. 2, in legacy mobile networks, such as GSM, the information on the serving MSC/VLR (stored in the HLR) is adequate. That is, the called party can be reached even after the loss of the subscriber location area (LA) infor-

4

mation by a searching/paging mechanism. In step 1, the current V-MSC/VLR for a called party is first located and in step 2 a setup toward the V-MSC/VLR is performed. In step 3, upon a loss of the LA information, the called party is paged in all cells under the V-MSC/VLR.

On the other hand, as illustrated in FIG. 3, in the 3G All-IP network, no such searching mechanism is available, so that the information of the current S-CSCF (stored in the HSS) is insufficient to reach the subscriber upon the loss of the subscriber TA. In step 1, S-CSCF is located and in step 2 a setup toward the S-CSCF is performed. However, in step 3, in the absence of the TA of the called party, the called party is not reachable.

The applicants have determined that the TA of a 3G All-IP subscriber should be protected against loss with the same level of security as that for the Serving CSCF (S-CSCF). The applicants have proposed options to protect the TA of a subscriber, namely, one option in which the TA is forwarded to the HSS and another option in which there is a security backup of the TA within the CSCF. The TA of the subscriber should be forwarded to the HSS at registration and downloaded from the HSS to the S-CSCF during recovery. Still another option is to have a permanent IPv6 (Internet Protocol Version 6) address allocated to the subscriber and to have the subscriber update its current Care-of Address (part of the TA) to the Home Agent upon obtaining the current TA.

As noted above, in accordance with the present disclosure, various options are available for implementing protection and recovery of the subscriber TA.

In the first option, as illustrated in FIG. 4A, “a safe copy” of the subscriber’s TA is forwarded to the HSS for storage and protection. The TA must enjoy the same level of protection against loss as the S-CSCF address. The TA and other data can then be restored to the S-CSCF upon the earlier loss of the data by the S-CSCF. It is noted that the subscriber’s TA is stored in the S-CSCF for normal operation. An incoming call from an REP (Remote End-Point) is received by the S-CSCF in step 1. In step 2, the S-CSCF looks for the subscriber’s TA so as to route the call but fails to find the subscriber’s TA. In step 3, the S-CSCF initiates the restoration of the subscriber’s TA (and possibly other data) from the HSS. This option is only available when the S-CSCF loses only the TA of the subscriber. Finally, in step 4, the call is then routed to the subscriber using the recovered TA.

As illustrated in FIG. 4B in step 1, the registering subscriber forwards an AL registration request to the S-CSCF including the TA. In step 2, an AL Location Update is forwarded to the HSS including the TA and S-CSCF address. In step 3, the HSS stores the updated TA and S-CSCF address (in a hard disk, for example, or other non-volatile memory). In step 4, the HSS forwards an AL Location Update acknowledgement to the S-CSCF which stores the TA and subscription profile and other data in step 5. In step 6, the S-CSCF forwards an AL registration acknowledge to the registering subscriber.

In the second option, the same level of protection against loss applies for the subscriber’s TA stored in the S-CSCF as that of the S-CSCF address stored in the HSS. For example, the subscriber’s TA can be backed up in a hard disk, or other non-volatile memory in the S-CSCF.

In the case of an S-CSCF crash, when the S-CSCF restarts, all of the information regarding the mobile subscribers registered with it, including the information on how to reach the mobile subscribers, is lost. In such a situation, it is not possible to deliver mobile terminated calls to the mobile subscribers that were registered with the S-CSCF that was restarted.

US 7,937,081 B2

5

In providing a solution to the above-noted problem in accordance with the third option, the following assumptions are made:

1) IPv6 is adopted for IP addressing and a subscriber is given a home address at subscription time. This home address is stored in a UMS.

2) The subscriber is in an area assigned to an S-CSCF and has registered with it and has provided its' TA, that is, the current address where the subscriber is reachable. Such an address is not the static home address but rather is the Care-of Address. Whenever the S-CSCF has to forward signaling to the mobile subscriber, it uses the Care-of Address. The subscriber has also registered its current Care of Address with its Home Agent.

3) The S-CSCF restarts due to a fault and loses the information about the mobile station.

The following procedure in accordance with the present disclosure, as illustrated in FIG. 5, may, for example, be used for mobile terminating call delivery when, as illustrated in 1, the S-CSCF crashes and restarts, the S-CSCF has no memory of what mobile stations (MSs) were registered with the S-CSCF and does not have any of the MSs Care of Address addresses:

When an incoming call at 2 reaches a CSCF in the home network, either from another IP based terminal or from an MGCF (Media Gateway Control Function), the I-CSCF queries at 3 the UMS based on the alias dialed by the calling party.

During registration, the UMS has stored information about the S-CSCF and information as to how the mobile subscriber can be reached. More particularly, the UMS has stored the address of the S-CSCF, that is, the address where CC (Call Control) signaling must be forwarded. At this point, two scenarios are possible:

The information in the UMS regarding the S-CSCF is still valid; the UMS returns at 4 the address of the S-CSCF and the Subscriber Identity and then forwards the call setup 5 to the S-CSCF.

The S-CSCF, not having information available for the alias to which the call corresponds due to a crash, queries 6 the UMS based on the Subscriber Identity optionally indicating that a restart took place in order to trigger a profile download.

The UMS returns at 7 the Home Address of the MS to the S-CSCF.

The S-CSCF forwards at 8 the signaling to the Home Address which is the home agent.

The home agent receives the packets at 9 and forwards them at 10 to the MS using the Care of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the MS receives the first packet, it sends at 11 a message to the S-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP) and call control signalling is sent at 12 from the S-CSCF to the MS.

When the call is terminated the subscriber can optionally re-register with the S-CSCF.

2) The information in the UMS is not valid; the UMS returns the Home Address of the mobile subscriber.

The I-CSCF forwards the signaling to the Home Address. The Home Agent receives the packets and forwards them to the Care-of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

6

When the mobile subscriber receives the first packet, it sends a message to the I-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP).

When the call is terminated the subscriber can optionally re-register with a S-CSCF.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, drawings, and appended claims without departing from the spirit of the invention. For example, the example embodiments of the present invention have been described with respect to currently used networks, such as 3G All-IP mobile networks, and standards for simplicity. It is, of course, understood that the present invention is not limited thereto. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

1. A method comprising:

receiving a call for a subscriber at an Interrogating-Call State Control Function (I-CSCF);  
sending a route request from the I-CSCF to a User Mobility Server (UMS);  
receiving an address of a Server-Call State Control Function (S-CSCF) at the I-CSCF from the UMS; and  
sending a call setup request from the I-CSCF to the S-CSCF.

2. The method of claim 1, wherein said sending a route request comprises querying the UMS based on an alias of the subscriber which was dialed by a party that sent the call.

3. The method of claim 1, further comprising receiving an identity of the subscriber at the I-CSCF from the UMS.

4. The method of claim 3, wherein the call setup request includes the identity of the subscriber.

5. The method of claim 1, wherein said receiving an address of a S-CSCF and said sending a call setup request are performed only if information about the S-CSCF stored in the UMS is valid.

6. The method of claim 5, further comprising, in response to the information about the S-CSCF stored in the UMS being invalid, receiving a home address of the subscriber at the I-CSCF from the UMS and sending the home address to a home agent corresponding to the home address of the subscriber.

7. A method comprising:

receiving a call setup request for a subscriber at a Serving-Call State Control Function (S-CSCF);  
sending a route request from the S-CSCF to a User Mobility Server (UMS);  
receiving a home address of the subscriber at the S-CSCF from the UMS; and  
sending the call setup request from the S-CSCF to a home agent at the home address of the subscriber.

8. The method of claim 7, wherein the call setup request includes a subscriber identity associated with the subscriber.

9. The method of claim 8, wherein said sending a route request comprises querying the UMS based on the subscriber identity.

US 7,937,081 B2

7

10. The method of claim 7, wherein the route request is configured to trigger a download to the S-CSCF of information associated with the subscriber.

11. The method of claim 10, wherein said sending a route request includes an indication to the UMS that the S-CSCF does not have a care of address of the subscriber.

12. The method of claim 7, further comprising receiving a registration request at the S-CSCF from the subscriber after said sending the call setup request.

13. The method of claim 7, wherein said sending the call setup request comprises sending the call setup request to a care of address of the subscriber.

14. A tangible computer-readable medium having instructions stored thereon, the instructions comprising:

instructions for receiving a call for a subscriber at an Interrogating-Call State Control Function (I-CSCF);

instructions for sending a route request from the I-CSCF to a User Mobility Server (UMS);

instructions for receiving an address of a Server-Call State Control Function (S-CSCF) at the I-CSCF from the UMS; and

instructions for sending a call setup request from the I-CSCF to the S-CSCF.

15. The tangible computer-readable medium of claim 14, wherein said instructions for sending a route request comprises instructions for querying the UMS based on an alias of the subscriber which was dialed by a party that sent the call.

16. The tangible computer-readable medium of claim 14, further comprising instructions for receiving an identity of the subscriber at the I-CSCF from the UMS.

17. The tangible computer-readable medium of claim 16, wherein the call setup request includes the identity of the subscriber.

18. The tangible computer-readable medium of claim 14, wherein said instructions for receiving an address of a S-CSCF and said instructions for sending a call setup request are executed only if information about the S-CSCF stored in the UMS is valid.

19. The tangible computer-readable medium of claim 18, further comprising instructions for receiving a home address of the subscriber at the I-CSCF from the UMS and instructions for sending the home address to a home agent corresponding to the home address of the subscriber.

20. A tangible computer-readable medium having instructions stored thereon, the instructions comprising:

instructions for receiving a call setup request for a subscriber at a Serving-Call State Control Function (S-CSCF);

instructions for sending a route request from the S-CSCF to a User Mobility Server (UMS);

instructions for receiving a home address of the subscriber at the S-CSCF from the UMS; and

instructions for sending the call setup request from the S-CSCF to a home agent at the home address of the subscriber.

21. The tangible computer-readable medium of claim 20, wherein the call setup request includes a subscriber identity associated with the subscriber.

22. The tangible computer-readable medium of claim 21, wherein said instructions for sending a route request comprises instructions for querying the UMS based on the subscriber identity.

23. The tangible computer-readable medium of claim 20, wherein the route request is configured to trigger a download to the S-CSCF of information associated with the subscriber.

8

24. The tangible computer-readable medium of claim 20, wherein the route request includes an indication to the UMS that the S-CSCF does not have a care of address of the subscriber.

25. The tangible computer-readable medium of claim 20, further comprising instructions for receiving a registration request at the S-CSCF from the subscriber.

26. The tangible computer-readable medium of claim 20, wherein said instructions for sending the call setup request comprises instructions for sending the call setup request to a care of address of the subscriber.

27. A system comprising:

an Interrogating-Call State Control Function (I-CSCF) configured to:

receive a call for a subscriber;

send a first route request to a User Mobility Server (UMS);

receive an address of a Server-Call State Control Function (S-CSCF) from the UMS; and

send a call setup request to the S-CSCF; and

the S-CSCF configured to:

receive the call setup request from the I-CSCF;

send a second route request to the UMS;

receive a home address of the subscriber from the UMS; and

send the call setup request to a home agent at the home address of the subscriber.

28. The system of claim 27, wherein the I-CSCF is further configured to query the UMS based on an alias of the subscriber which was dialed by a party that sent the call.

29. The system of claim 27, wherein the I-CSCF is further configured to receive an identity of the subscriber from the UMS.

30. The system of claim 29, wherein the call setup request includes the identity of the subscriber.

31. The system of claim 30, wherein the S-CSCF is further configured to query the UMS based on the identity of the subscriber.

32. The system of claim 27, wherein the I-CSCF is configured to receive the address of the S-CSCF and to send the call setup request to the S-CSCF only if information about the S-CSCF stored in the UMS is valid.

33. The system of claim 32, wherein the I-CSCF is further configured to, in response to the information about the S-CSCF stored in the UMS being invalid, receive a home address of the subscriber from the UMS and send the home address to the home agent corresponding to the home address of the subscriber.

34. The system of claim 27, wherein the second route request is configured to trigger a download to the S-CSCF of information associated with the subscriber.

35. The system of claim 34, wherein the second route request includes an indication to the UMS that the S-CSCF does not have a care of address of the subscriber.

36. The system of claim 27, wherein the S-CSCF is further configured to receive a registration request at the S-CSCF from the subscriber.

37. The system of claim 27, wherein the S-CSCF is further configured to send the call setup request to a care of address of the subscriber.

38. The system of claim 27, further comprising the home agent, wherein the home agent is configured to receive the call setup request from the S-CSCF and forward the call setup request to a care of address of the subscriber.

\* \* \* \* \*



UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,937,081 B2  
APPLICATION NO. : 12/720862  
DATED : May 3, 2011  
INVENTOR(S) : Phan-Anh et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 1, line 7, delete "Division" and insert -- Divisional --.

Signed and Sealed this  
Thirtieth Day of August, 2011

A handwritten signature in black ink that reads "David J. Kappos". The signature is written in a cursive, flowing style with a large initial "D" and a stylized "K".

David J. Kappos  
*Director of the United States Patent and Trademark Office*

US007937081C1

(12) **INTER PARTES REEXAMINATION CERTIFICATE (1332nd)**  
**United States Patent**  
**Phan-Anh et al.**

(10) **Number:** **US 7,937,081 C1**(45) **Certificate Issued:** **Aug. 19, 2016**(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

(75) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Helsinki (FI); **Stefano Faccin**, Dallas, TX (US)

(73) Assignee: **INTELLECTUAL VENTURES I LLC**, Wilmington, DE (US)

**Reexamination Request:**

No. 95/001,899, Feb. 17, 2012

**Reexamination Certificate for:**

Patent No.: **7,937,081**  
 Issued: **May 3, 2011**  
 Appl. No.: **12/720,862**  
 Filed: **Mar. 10, 2010**

Certificate of Correction issued Aug. 30, 2011

**Related U.S. Application Data**

(62) Division of application No. 09/802,861, filed on Mar. 12, 2001, now Pat. No. 7,769,374.

(51) **Int. Cl.**

**H04W 24/00** (2009.01)  
**H04W 8/12** (2009.01)  
**H04W 60/00** (2009.01)  
**H04W 8/26** (2009.01)  
**H04W 24/02** (2009.01)  
**H04W 24/04** (2009.01)

(52) **U.S. Cl.**

CPC ..... **H04W 8/26** (2013.01); **H04W 24/02** (2013.01); **H04W 24/04** (2013.01)

(58) **Field of Classification Search**

None

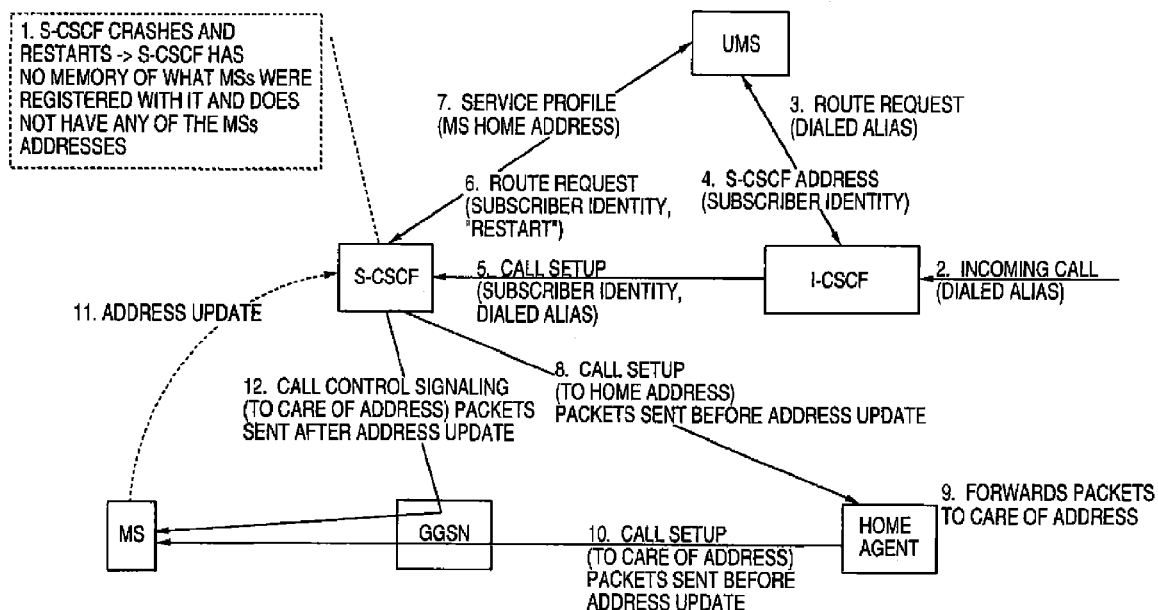
See application file for complete search history.

(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 95/001,899, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

*Primary Examiner* — Minh Dieu Nguyen(57) **ABSTRACT**

A technique for protecting location information of a subscriber in a mobile network is disclosed which forwards a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding a location update from the S-CSCF to an HSS including the subscriber's TA. Upon the S-CSCF losing data, lost data may be restored to the S-CSCF from the data stored in the HSS. The HSS may store data in a non-volatile memory such as a hard disk drive. The technique may also include forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding a location update from the S-CSCF to an HSS and storing data in a non-volatile memory such as a hard disk drive in the S-CSCF so as to be protected against loss. Upon the S-CSCF losing data, lost data including the subscriber's TA may be restored to the S-CSCF from the data stored in the S-CSCF.





US 7,937,081 C1

1

2

**INTER PARTES  
REEXAMINATION CERTIFICATE**

THE PATENT IS HEREBY AMENDED AS 5  
INDICATED BELOW.

AS A RESULT OF REEXAMINATION, IT HAS BEEN  
DETERMINED THAT:

The patentability of claims **30** and **31** is confirmed. 10  
Claims **1, 5, 7-9, 13-14, 18, 20-22, 26-27, 32** and **37-38**  
are cancelled.

Claims **2-4, 6, 10-12, 15-17, 19, 23-25, 28-29** and **33-36**  
were not reexamined. 15

\* \* \* \* \*

# Exhibit P

---

(12) **United States Patent**  
**Phan-Anh et al.**

(10) **Patent No.:** **US 8,200,211 B2**  
(45) **Date of Patent:** **\*Jun. 12, 2012**

(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

(75) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Helsinki (FI); **Stefano Faccin**, Dallas, TX (US)

(73) Assignee: **Intellectual Ventures I LLC**, Wilmington, DE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/097,709**

(22) Filed: **Apr. 29, 2011**

(65) **Prior Publication Data**

US 2011/0199978 A1 Aug. 18, 2011

**Related U.S. Application Data**

(60) Continuation of application No. 12/720,862, filed on Mar. 10, 2010, now Pat. No. 7,937,081, which is a division of application No. 09/802,861, filed on Mar. 12, 2001, now Pat. No. 7,769,374.

(51) **Int. Cl.**  
**H04W 24/00** (2009.01)

(52) **U.S. Cl.** ..... **455/424; 455/415; 455/433; 370/328; 370/338**

(58) **Field of Classification Search** ..... **455/424, 455/415, 433; 370/328, 338**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS			
5,077,830	A	12/1991	Mallia
5,463,672	A	10/1995	Kage
5,561,854	A	10/1996	Antic et al.
6,097,942	A	8/2000	Laiho
6,163,532	A	12/2000	Taguchi et al.
6,408,182	B1	6/2002	Davidson et al.
6,411,632	B2	6/2002	Lindgren et al.
6,445,911	B1	9/2002	Chow et al.
6,587,882	B1	7/2003	Inoue et al.
6,594,490	B1	7/2003	Toyoda et al.
6,600,920	B1	7/2003	Stephens et al.
6,636,491	B1	10/2003	Kari et al.
6,654,606	B1	11/2003	Foti et al.
6,707,813	B1	3/2004	Hasan et al.
6,721,291	B1	4/2004	Bergenwall et al.
6,732,177	B1	5/2004	Roy
6,763,233	B2	7/2004	Bharatia
6,775,255	B1	8/2004	Roy
6,839,323	B1	1/2005	Foti

(Continued)

**OTHER PUBLICATIONS**

International Preliminary Examination Report for PCT/IB02/00721 completed Apr. 3, 2003.

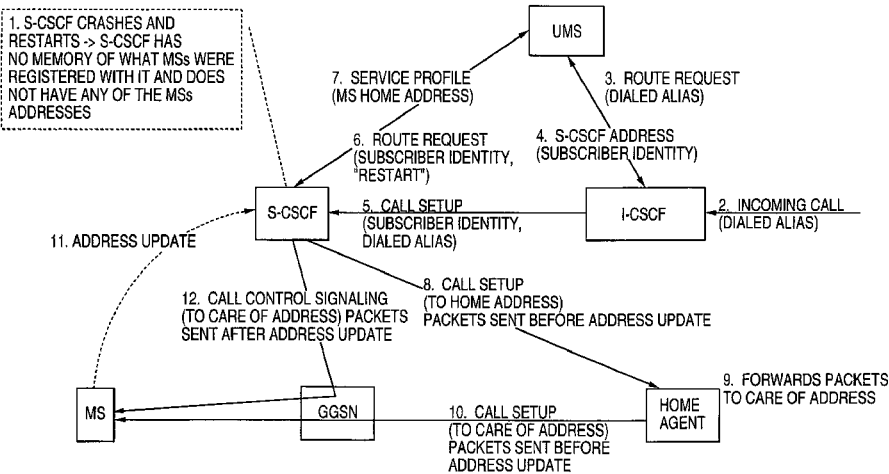
(Continued)

Primary Examiner — Nghi Ly

(57) **ABSTRACT**

A technique for protecting location information of a subscriber in a mobile network is disclosed. A User Mobility Server (UMS) receives a first query from a first call state control function (CSCF). The UMS transmits a call setup and a subscriber identity to a servicing-call state control function (S-CSCF). The S-CSCF may have no record of the subscriber identity due to a restart or some other event. The UMS receives a second query from the S-CSCF based in part of the subscriber identity. The UMS transmits a home address of a mobile station to the S-CSCF. The UMS may also transmit a profile download to the S-CSCF.

**21 Claims, 6 Drawing Sheets**



**US 8,200,211 B2**

Page 2

---

U.S. PATENT DOCUMENTS

7,006,449 B2 \* 2/2006 Teraoka ..... 370/252  
7,602,762 B1 10/2009 Kauppinen et al.  
7,937,081 B2 \* 5/2011 Phan-Anh et al. .... 455/424

OTHER PUBLICATIONS

International Search Report for PCT/IB02/00721, mailed Feb. 26, 2003.

Notice of Allowance on U.S. Appl. No. 12/720,862, mailed Dec. 27, 2010.

Non-Final Office Action on U.S. Appl. No. 12/720,862, mailed Jul. 8, 2010.

Technical Report TR 23.821 V1.0.1, published Jul. 2000 by the 3rd Generation partnership Project 3GPP.

\* cited by examiner

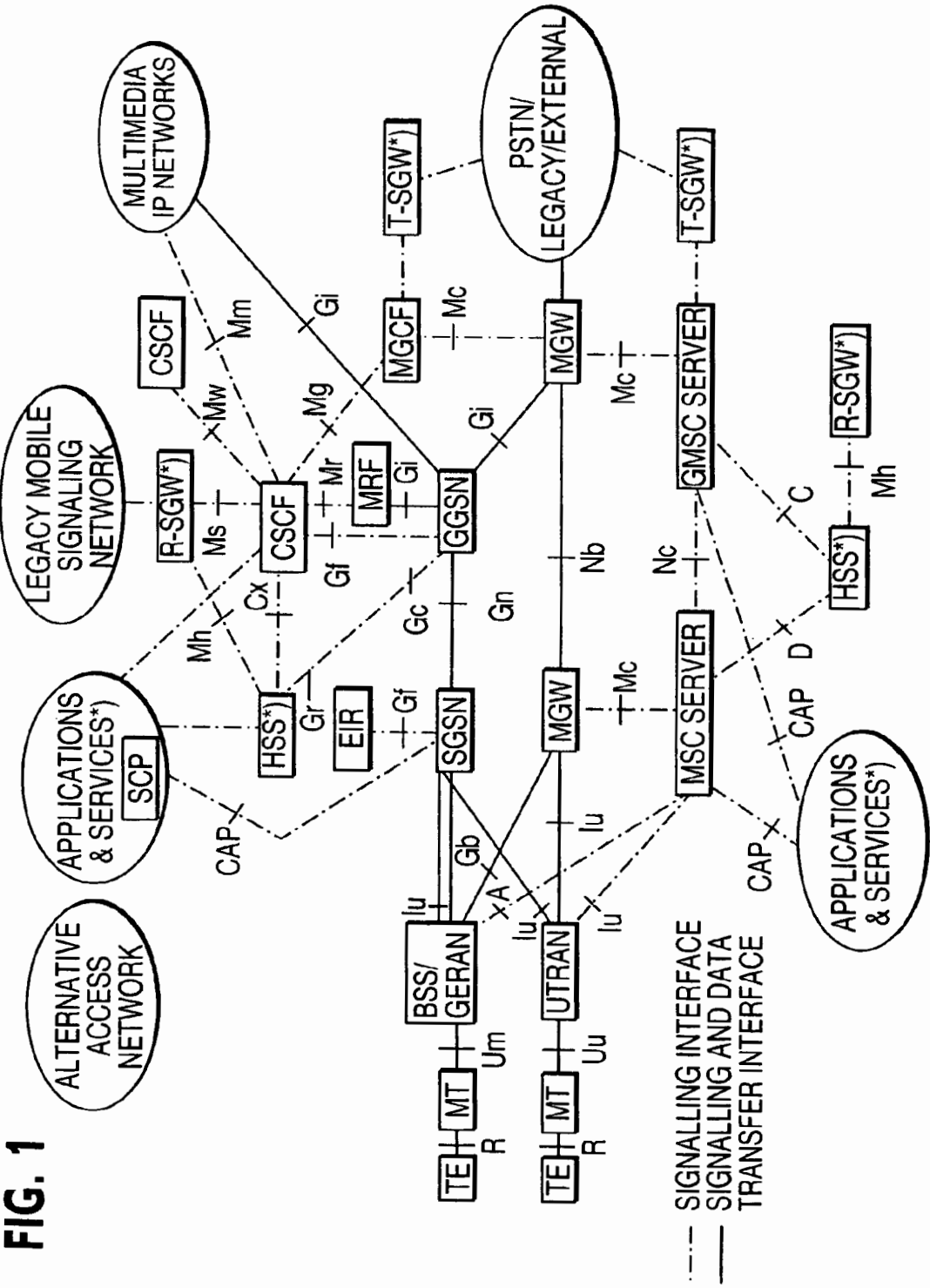


FIG. 2

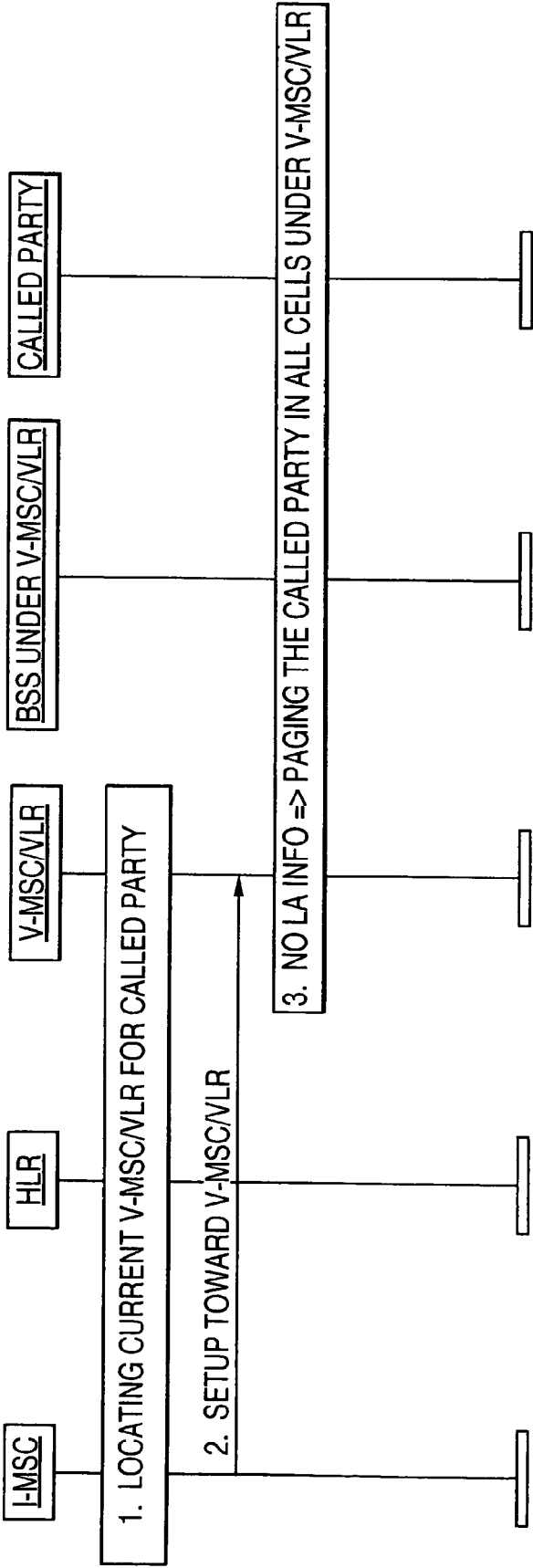




FIG. 3

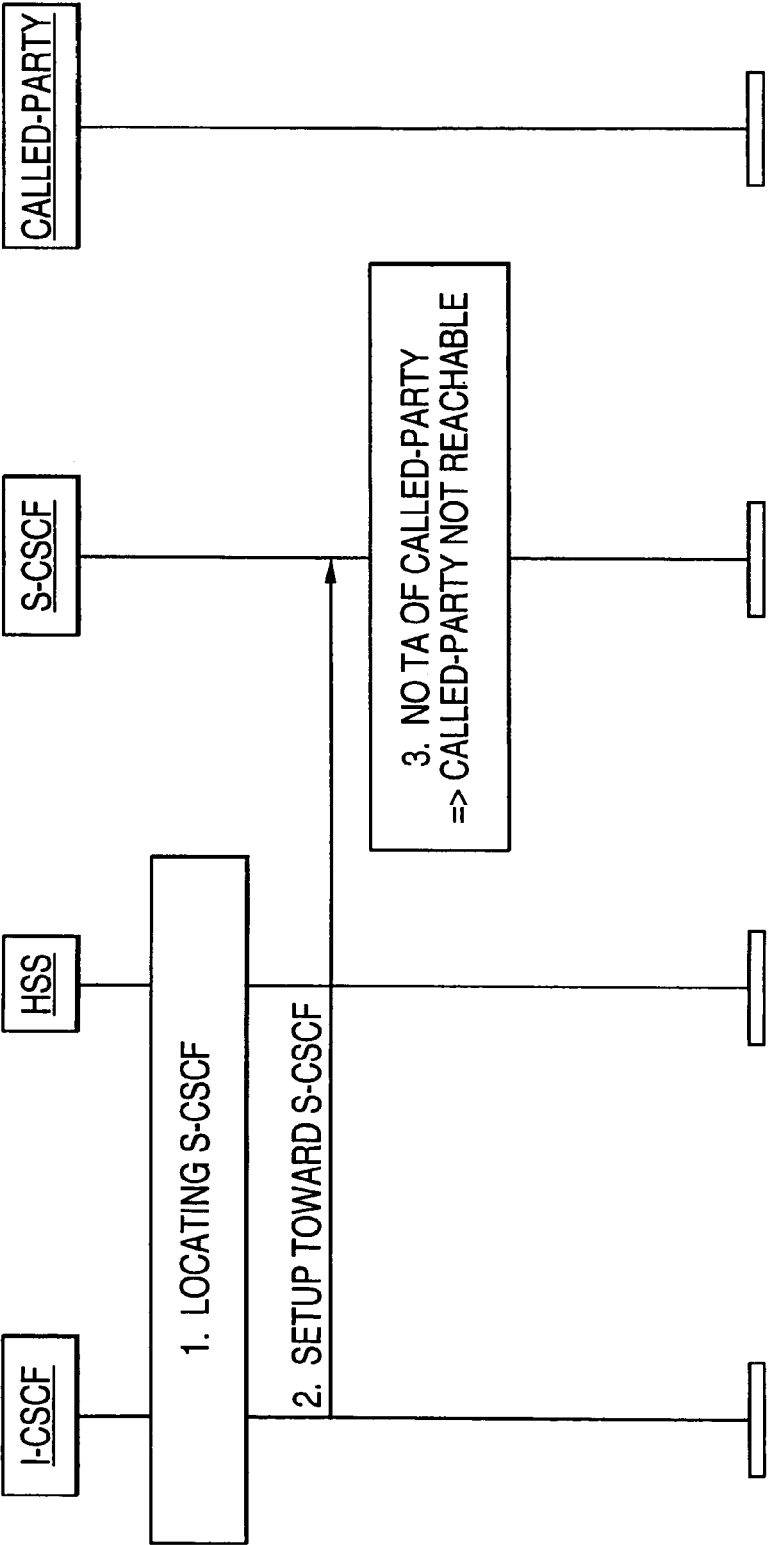


FIG. 4A

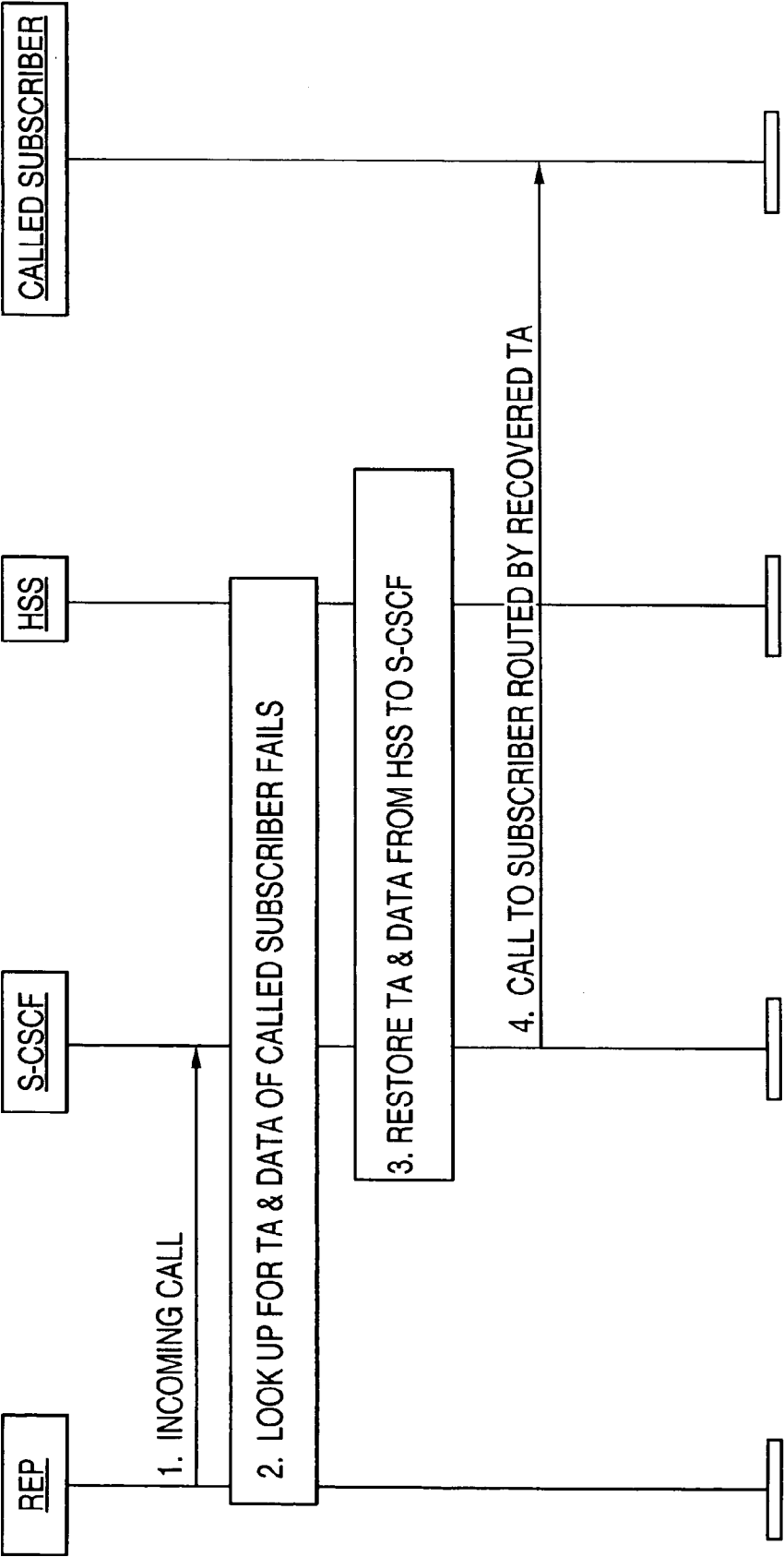


FIG. 4B

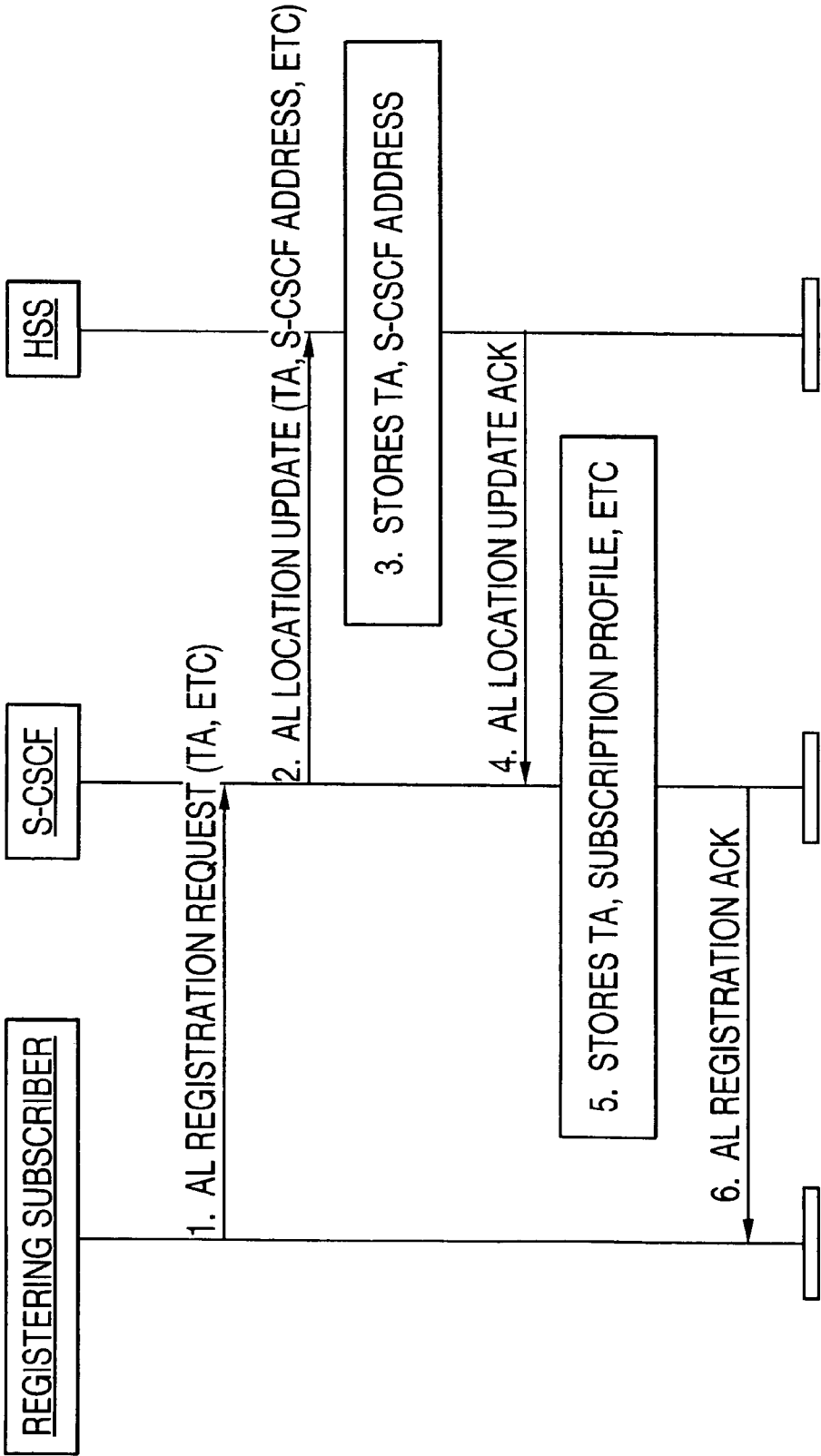
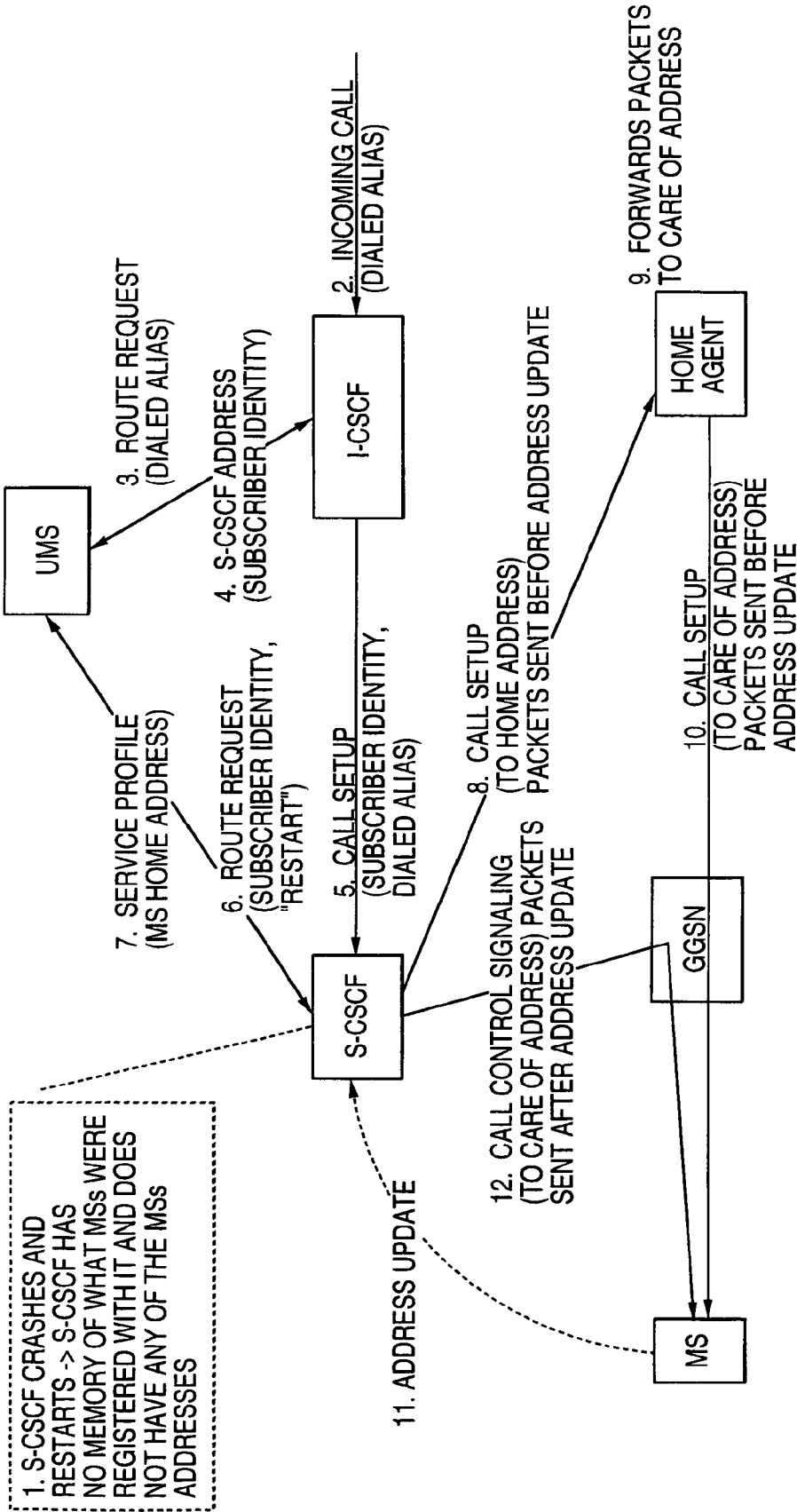


FIG. 5



US 8,200,211 B2

1

**RECOVERY TECHNIQUES IN MOBILE NETWORKS****CROSS-REFERENCE TO RELATED PATENT APPLICATIONS**

This application is a Continuation of U.S. patent application Ser. No. 12/720,862, filed Mar. 10, 2010, which is a Divisional of U.S. patent application Ser. No. 09/802,861, filed Mar. 12, 2001, (now U.S. Pat. No. 7,769,374), both of which are incorporated herein by reference in their entirety.

**FIELD**

The present disclosure relates to recovery techniques for use in mobile networks. More particularly, the present disclosure relates to protecting the Transport Address (TA) which is a current Care of Address of a mobile subscriber is reachable from loss and after Call State Control Function (CSCF) crashes and after reset situations of a network element realizing CSCF functionality.

**DESCRIPTION OF RELATED ART**

Technical Report TR 23.821 V1.0.1, published July 2000 by the 3rd Generation Partnership Project (3GPP) and available on the Internet at <http://www.3gpp.org>, discloses the specifications of a 3G All-IP mobile network and this report is incorporated by reference herein in its entirety.

FIG. 1 illustrates the architecture of the network disclosed in the above-noted Technical Report. The elements shown with asterisks are elements which have been duplicated for figure layout purposes only. These duplicated elements belong to the same logical element in the reference model.

Unfortunately, the network disclosed in the Technical Report fails to include any protection of the TA of a 3G All-IP subscriber from loss. Furthermore, the network disclosed in the Technical Report fails to protect the IP address of a subscriber in the case of a reset situation of a network element realizing CSCF functionality, that is, a CSCF, thereby preventing recovery after a reset of the network element. Still furthermore, the network disclosed in the Technical Report fails to protect the location information of a subscriber after a CSCF crash, thereby preventing recovery after a CSCF crash.

**SUMMARY**

An object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL (Application Level) location update from the S-CSCF to a Home Subscriber Server (HSS) including the subscriber's TA and the (S-CSCF) address and storing data including the subscriber's TA and the S-CSCF address in the HSS so as to be protected against loss.

Another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL location update from the S-CSCF to an HSS including the S-CSCF address and storing data including the subscriber's TA in a non-volatile memory of the S-CSCF so as to be protected against loss.

Yet another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including upon an S-CSCF receiving a

2

call setup request for the subscriber from an Interrogating Call State Control Function (I-CSCF), forwarding a route request to a User Mobility Server (UMS) and receiving a home address of the subscriber and then forwarding the call setup request from the S-CSCF to a home agent at the home address of the subscriber and then forwarding the call setup request from the home agent to the subscriber and subsequently forwarding an address update from the subscriber to the S-CSCF.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing and a better understanding of the present disclosure will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this disclosure. While the foregoing and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, issued a clearly understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 illustrates the architecture of a 3G All-IP mobile network.

FIG. 2 illustrates reaching a called party after losing LA (Location Area) information in a legacy mobile network.

FIG. 3 illustrates failure to reach a called party after losing TA information in a 3GPP All-IP mobile network.

FIG. 4A illustrates sending subscriber TA to S-CSCF and then forwarding it to HSS at registration.

FIG. 4B illustrates an example of reaching a called party after losing TA information in a mobile network in accordance with the present disclosure.

FIG. 5 illustrates the signal flow in the case of a recovery after a CSCF crash in accordance with another embodiment of the present disclosure.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Before beginning a detailed description of the subject disclosure, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, other components may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

In the application level of a 3G All-IP network, the reachability of a subscriber is maintained in two levels, namely, the network element level and the subscriber level. The S-CSCF that the subscriber is currently registered to and the TA of the roaming subscriber, which the subscriber provides to the network during Application Level (AL) registration, must be known to and maintained by the network.

Without specific support for mobility in IPv6, packets destined to a mobile subscriber would not be able to reach it while the subscriber is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a subscriber could change its IP address each time

US 8,200,211 B2

3

it moves to a new link, but it would then not be able to maintain transport and higher-layer connections when it changes location.

Mobile IPv6 allows a subscriber to move from one link to another without changing its IP address. A subscriber is always addressable by its “home address”, an IP address assigned to it within its home subnet prefix on its home link. Packets may be routed to the subscriber using this address regardless of its current point of attachment to the Internet, and it may continue to communicate with others after moving to a new link. The movement of a subscriber away from its home link is thus transparent to transport and higher-layer protocols and applications.

A mobile subscriber is always addressable by its home address, whether it is currently attached to its home link or is away from home. While it is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if it were never mobile. Since the subnet prefix of its home address is the subnet prefix (or one of the subnet prefixes) on the subscribers’ home link (it is the mobile subscribers’ home subnet prefix), packets addressed to it will be routed to its home link.

While a subscriber is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while the subscriber is visiting a particular foreign link. The subnet prefix of a subscriber’s care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by it; if it is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the subscriber in its location away from home.

The association between a subscriber’s home address and care-of address is known as a “binding” for the subscriber. It typically acquires its care-of address through stateless or stateful Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static preassignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this discussion.

While away from home, a mobile subscriber registers one of its care-of addresses with a router on its home link, requesting this router to function as the “home agent” for it. This binding registration is done by the subscriber sending to the home agent a packet containing a “Binding Update” destination option; the home agent then replies to the subscriber by returning a packet containing a “Binding Acknowledgment” destination option. The care-of address in this binding registered with its home agent is known as the subscriber’s “primary care-of address”. The subscribers’ home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the subscribers’ home address (or home addresses) on the home link and tunnels each intercepted packet to the subscribers’ primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation, with the outer IPv6 header addressed to the subscribers’ primary care-of address.

Keeping the address of the S-CSCF ensures that a call to a subscriber can be routed to the destination node, that is, the S-CSCF. Keeping the current TA of the subscriber ensures that a call made to the subscriber which arrives at the S-CSCF can finally reach the subscriber.

As illustrated in FIG. 2, in legacy mobile networks, such as GSM, the information on the serving MSC/VLR (stored in the HLR) is adequate. That is, the called party can be reached even after the loss of the subscriber location area (LA) infor-

4

mation by a searching/paging mechanism. In step 1, the current V-MSC/VLR for a called party is first located and in step 2 a setup toward the V-MSC/VLR is performed. In step 3, upon a loss of the LA information, the called party is paged in all cells under the V-MSC/VLR.

On the other hand, as illustrated in FIG. 3, in the 3G All-IP network, no such searching mechanism is available, so that the information of the current S-CSCF (stored in the HSS) is insufficient to reach the subscriber upon the loss of the subscriber TA. In step 1, S-CSCF is located and in step 2 a setup toward the S-CSCF is performed. However, in step 3, in the absence of the TA of the called party, the called party is not reachable.

The applicants have determined that the TA of a 3G All-IP subscriber should be protected against loss with the same level of security as that for the Serving CSCF (S-CSCF). The applicants have proposed options to protect the TA of a subscriber, namely, one option in which the TA is forwarded to the HSS and another option in which there is a security backup of the TA within the CSCF. The TA of the subscriber should be forwarded to the HSS at registration and downloaded from the HSS to the S-CSCF during recovery. Still another option is to have a permanent IPv6 (Internet Protocol Version 6) address allocated to the subscriber and to have the subscriber update its current Care-of Address (part of the TA) to the Home Agent upon obtaining the current TA.

As noted above, in accordance with the present disclosure, various options are available for implementing protection and recovery of the subscriber TA.

In the first option, as illustrated in FIG. 4A, “a safe copy” of the subscriber’s TA is forwarded to the HSS for storage and protection. The TA must enjoy the same level of protection against loss as the S-CSCF address. The TA and other data can then be restored to the S-CSCF upon the earlier loss of the data by the S-CSCF. It is noted that the subscriber’s TA is stored in the S-CSCF for normal operation. An incoming call from an REP (Remote End-Point) is received by the S-CSCF in step 1. In step 2, the S-CSCF looks for the subscriber’s TA so as to route the call but fails to find the subscriber’s TA. In step 3, the S-CSCF initiates the restoration of the subscriber’s TA (and possibly other data) from the HSS. This option is only available when the S-CSCF loses only the TA of the subscriber. Finally, in step 4, the call is then routed to the subscriber using the recovered TA.

As illustrated in FIG. 4B in step 1, the registering subscriber forwards an AL registration request to the S-CSCF including the TA. In step 2, an AL Location Update is forwarded to the HSS including the TA and S-CSCF address. In step 3, the HSS stores the updated TA and S-CSCF address (in a hard disk, for example, or other non-volatile memory). In step 4, the HSS forwards an AL Location Update acknowledgement to the S-CSCF which stores the TA and subscription profile and other data in step 5. In step 6, the S-CSCF forwards an AL registration acknowledge to the registering subscriber.

In the second option, the same level of protection against loss applies for the subscriber’s TA stored in the S-CSCF as that of the S-CSCF address stored in the HSS. For example, the subscriber’s TA can be backed up in a hard disk, or other non-volatile memory in the S-CSCF.

In the case of an S-CSCF crash, when the S-CSCF restarts, all of the information regarding the mobile subscribers registered with it, including the information on how to reach the mobile subscribers, is lost. In such a situation, it is not possible to deliver mobile terminated calls to the mobile subscribers that were registered with the S-CSCF that was restarted.



## US 8,200,211 B2

5

In providing a solution to the above-noted problem in accordance with the third option, the following assumptions are made:

1) IPv6 is adopted for IP addressing and a subscriber is given a home address at subscription time. This home address is stored in a UMS.

2) The subscriber is in an area assigned to an S-CSCF and has registered with it and has provided its TA, that is, the current address where the subscriber is reachable. Such an address is not the static home address but rather is the Care-of Address. Whenever the S-CSCF has to forward signaling to the mobile subscriber, it uses the Care-of Address. The subscriber has also registered its current Care of Address with its Home Agent.

3) The S-CSCF restarts due to a fault and loses the information about the mobile station.

The following procedure in accordance with the present disclosure, as illustrated in FIG. 5, may, for example, be used for mobile terminating call delivery when, as illustrated in 1, the S-CSCF crashes and restarts, the S-CSCF has no memory of what mobile stations (MSs) were registered with the S-CSCF and does not have any of the MSs Care of Address addresses:

When an incoming call at 2 reaches a CSCF in the home network, either from another IP based terminal or from an MGCF (Media Gateway Control Function), the I-CSCF queries at 3 the UMS based on the alias dialed by the calling party.

During registration, the UMS has stored information about the S-CSCF and information as to how the mobile subscriber can be reached. More particularly, the UMS has stored the address of the S-CSCF, that is, the address where CC (Call Control) signaling must be forwarded. At this point, two scenarios are possible:

The information in the UMS regarding the S-CSCF is still valid; the UMS returns at 4 the address of the S-CSCF and the Subscriber Identity and then forwards the call setup 5 to the S-CSCF.

The S-CSCF, not having information available for the alias to which the call corresponds due to a crash, queries 6 the UMS based on the Subscriber Identity optionally indicating that a restart took place in order to trigger a profile download.

The UMS returns at 7 the Home Address of the MS to the S-CSCF.

The S-CSCF forwards at 8 the signaling to the Home Address which is the home agent.

The home agent receives the packets at 9 and forwards them at 10 to the MS using the Care of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the MS receives the first packet, it sends at 11 a message to the S-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP) and call control signalling is sent at 12 from the S-CSCF to the MS.

When the call is terminated the subscriber can optionally re-register with the S-CSCF.

2) The information in the UMS is not valid; the UMS returns the Home Address of the mobile subscriber.

The I-CSCF forwards the signaling to the Home Address. The Home Agent receives the packets and forwards them to the Care-of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

6

When the mobile subscriber receives the first packet, it sends a message to the I-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP).

When the call is terminated the subscriber can optionally re-register with a S-CSCF.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, drawings, and appended claims without departing from the spirit of the invention. For example, the example embodiments of the present invention have been described with respect to currently used networks, such as 3G All-IP mobile networks, and standards for simplicity. It is, of course, understood that the present invention is not limited thereto. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

1. A method comprising:

receiving a first query at a user mobility server (UMS) from a first call state control function (CSCF);  
transmitting a call setup and a subscriber identity (SI) to a servicing-call state control function (S-CSCF) from the UMS;

receiving a second query at the UMS from the S-CSCF based at least in part on the SI; and  
transmitting a home address of a mobile station to the S-CSCF from the UMS.

2. The method of claim 1, where the second query indicates that a restart took place at the S-CSCF.

3. The method of claim 2, further comprising transmitting a profile download to the S-CSCF from the UMS.

4. The method of claim 1, wherein the first query is a route request.

5. The method of claim 1, wherein the first query is based at least in part on an alias dialed by the mobile station.

6. The method of claim 5, wherein the mobile station is an internet protocol based terminal for which an internet protocol version 6 (IPv6) address is stored on the UMS.

7. The method of claim 1, further comprising transmitting an address of the S-CSCF and the SI from the UMS to the first CSCF.

8. A non-transitory computer readable medium having instructions stored thereon, the instructions comprising:

instructions for receiving a first query at a user mobility server (UMS) from a first call state control function (CSCF);

instructions for transmitting a call setup and a subscriber identity (SI) to a servicing-call state control function (S-CSCF) from the UMS;

instructions for receiving a second query at the UMS from the S-CSCF based at least in part on the SI; and  
instructions for transmitting a home address of a mobile station to the S-CSCF from the UMS.

9. The non-transitory computer readable medium of claim 8, where the second query indicates that a restart took place at the S-CSCF.

US 8,200,211 B2

7

10. The non-transitory computer readable medium of claim 9, further comprising instructions for transmitting a profile download to the S-CSCF from the UMS.

11. The non-transitory computer readable medium of claim 8, wherein the first query is a route request.

12. The non-transitory computer readable medium of claim 8, wherein the first query is based at least in part on an alias dialed by the mobile station.

13. The non-transitory computer readable medium of claim 12, wherein the mobile station is an internet protocol based terminal for which an internet protocol version 6 (IPV6) address is stored on the UMS.

14. The non-transitory computer readable medium of claim 8, further comprising instructions for transmitting an address of the S-CSCF and the SI from the UMS to the first CSCF.

15. A system comprising:  
an Interrogating-Call State Control Function (I-CSCF) configured to send a first query to a User Mobility Server (UMS);  
the UMS configured to:  
receive the first query from the I-CSCF,  
transmit a call setup and a subscriber identity (SI) to a servicing-call state control function (S-CSCF),

8

receive a second query from the S-CSCF based at least in part on the SI, and  
transmit a home address of a mobile station to the S-CSCF; and  
the S-CSCF configured to:  
receive the call setup from the UMS;  
transmit the second query to the UMS.

16. The system of claim 15, where the second query indicates that a restart took place at the S-CSCF.

17. The system of claim 16, wherein the UMS is further configured to transmit a profile download to the S-CSCF.

18. The system of claim 15, wherein the first query is a route request.

19. The system of claim 15, wherein the first query is based at least in part on an alias dialed by the mobile station.

20. The system of claim 19, wherein the mobile station is an internet protocol based terminal for which an internet protocol version 6 (IPV6) address is stored on the UMS.

21. The system of claim 15, wherein the UMS is further configured to transmit an address of the S-CSCF and the SI to the first CSCF.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 8,200,211 B2  
APPLICATION NO. : 13/097709  
DATED : June 12, 2012  
INVENTOR(S) : Phan-Anh et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

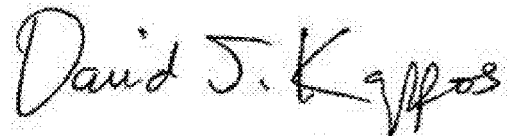
In Column 4, Line 3, delete “is.” and insert -- is --, therefor.

In Column 4, Line 12, delete “parry” and insert -- party --, therefor.

In Column 5, Line 24, delete “addresses:” and insert -- addresses. --, therefor.

In Column 6, Line 67, in Claim 9, delete “S-CS CF.” and insert -- S-CSCF. --, therefor.

Signed and Sealed this  
Twenty-third Day of October, 2012

A handwritten signature in black ink, reading "David J. Kappos". The signature is written in a cursive, flowing style with a large initial "D" and a stylized "K".

David J. Kappos  
*Director of the United States Patent and Trademark Office*

# Exhibit Q

---



US008600372B2

(12) **United States Patent**  
**Phan-Anh et al.**

(10) **Patent No.:** **US 8,600,372 B2**  
(45) **Date of Patent:** **\*Dec. 3, 2013**

(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

(71) Applicant: **Intellectual Ventures I LLC**, Bellevue, WA (US)

(72) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Espoo (FI); **Stefano Faccin**, Hayward, CA (US)

(73) Assignee: **Intellectual Ventures I LLC**, Wilmington, DE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/682,230**

(22) Filed: **Nov. 20, 2012**

(65) **Prior Publication Data**

US 2013/0165109 A1 Jun. 27, 2013

**Related U.S. Application Data**

(60) Continuation of application No. 13/484,583, filed on May 31, 2012, now Pat. No. 8,351,924, which is a continuation of application No. 13/097,709, filed on Apr. 29, 2011, now Pat. No. 8,200,211, which is a continuation of application No. 12/720,862, filed on Mar. 10, 2010, now Pat. No. 7,937,081, which is a division of application No. 09/802,861, filed on Mar. 12, 2001, now Pat. No. 7,769,374.

(51) **Int. Cl.**  
**H04W 24/00**

(2009.01)

(52) **U.S. Cl.**

USPC ..... **455/424**; 455/435.1; 455/415; 455/433

(58) **Field of Classification Search**

USPC ..... 455/424, 435.1, 415, 433  
See application file for complete search history.

(56)

**References Cited**

**U.S. PATENT DOCUMENTS**

5,077,830	A	12/1991	Mallia
5,274,694	A	12/1993	Lechner et al.
5,463,672	A	10/1995	Kage
5,561,854	A	10/1996	Antic et al.
6,097,942	A	8/2000	Laiho
6,163,532	A	12/2000	Taguchi et al.
6,408,182	B1	6/2002	Davidson et al.

(Continued)

**OTHER PUBLICATIONS**

International Preliminary Examination Report for PCT/IB02/00721 completed Apr. 3, 2003.

(Continued)

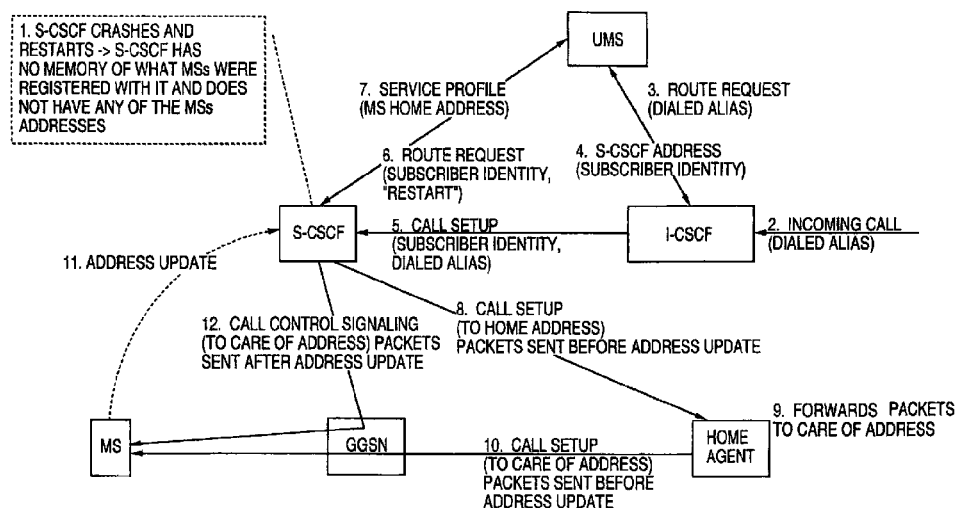
*Primary Examiner* — Nghi H Ly

(57)

**ABSTRACT**

A technique for protecting location information of a subscriber in a mobile network is disclosed. A User Mobility Server (UMS) receives a first query from a first call state control function (CSCF). The UMS transmits a call setup and a subscriber identity to a servicing-call state control function (S-CSCF). The S-CSCF may have no record of the subscriber identity due to a restart are some other event. The UMS receives a second query from the S-CSCF based in part of the subscriber identity. The UMS transmits a home address of a mobile station to the S-CSCF. The UMS may also transmit a profile download to the S-CSCF.

**15 Claims, 6 Drawing Sheets**



**US 8,600,372 B2**

Page 2

(56)

**References Cited****U.S. PATENT DOCUMENTS**

6,411,632	B2	6/2002	Lindgren et al.	
6,445,911	B1	9/2002	Chow et al.	
6,587,882	B1	7/2003	Inoue et al.	
6,594,490	B1	7/2003	Toyoda et al.	
6,600,920	B1	7/2003	Stephens et al.	
6,636,491	B1	10/2003	Kari et al.	
6,654,606	B1	11/2003	Foti et al.	
6,707,813	B1	3/2004	Hasan et al.	
6,721,291	B1	4/2004	Bergenwall et al.	
6,732,177	B1	5/2004	Roy	
6,763,233	B2	7/2004	Bharatia	
6,775,255	B1	8/2004	Roy	
6,839,323	B1	1/2005	Foti	
7,006,449	B2	2/2006	Teraoka	
7,221,940	B2 *	5/2007	Kaneko et al. ....	455/435.1
7,602,762	B1	10/2009	Kauppinen et al.	
7,769,374	B2	8/2010	Phan-Anh et al.	
7,937,081	B2	5/2011	Phan-Anh et al.	
8,200,211	B2	6/2012	Phan-Anh et al.	
2001/0031635	A1	10/2001	Bharatia	
2002/0147845	A1	10/2002	Sanchez-Herrero et al.	
2009/0029701	A1 *	1/2009	Mishima .....	455/435.1
2011/0076991	A1	3/2011	Mueck et al.	

**OTHER PUBLICATIONS**

International Search Report for PCT/IB02/00721, mailed Feb. 26, 2003.

Technical Report TR 23.821 V1.0.1, published Jul. 2000 by the 3<sup>rd</sup> Generation partnership Project 3GPP. 1-62 pages.

Notice of Allowance on U.S. Appl. No. 12/720,862, mailed Dec. 27, 2010.

Non-Final Office Action on U.S. Appl. No. 12/720,862, mailed Jul. 8, 2010.

Notice of Allowance on U.S. Appl. No. 09/802,861 mailed Nov. 25, 2009.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Aug. 3, 2009.

Re-Exam 95/001,899, filed May 31, 2012, Son Phan-Anh, et al.

Re-Exam 95/002,004, filed Aug. 6, 2012, Son Phan-Anh, et al.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Sep. 23, 2008.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Apr. 8, 2008.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Oct. 11, 2007.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed May 8, 2007.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Jun. 30, 2006.

Final Office Action on U.S. Appl. No. 09/802,861 mailed Apr. 6, 2005.

Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Nov. 28, 2003.

Notice of Allowance on U.S. Appl. No. 12/720,862 mailed Dec. 27, 2010.

Non-final Office Action on U.S. Appl. No. 12/720,862 mailed Jul. 8, 2010.

Notice of Allowance on U.S. Appl. No. 13/097,709 mailed Feb. 22, 2012.

Non-final Office Action on U.S. Appl. No. 13/097,709 mailed Sep. 1, 2011.

Notice of Allowance on U.S. Appl. No. 13/484583, mailed Sep. 12, 2012.

\* cited by examiner



FIG. 1

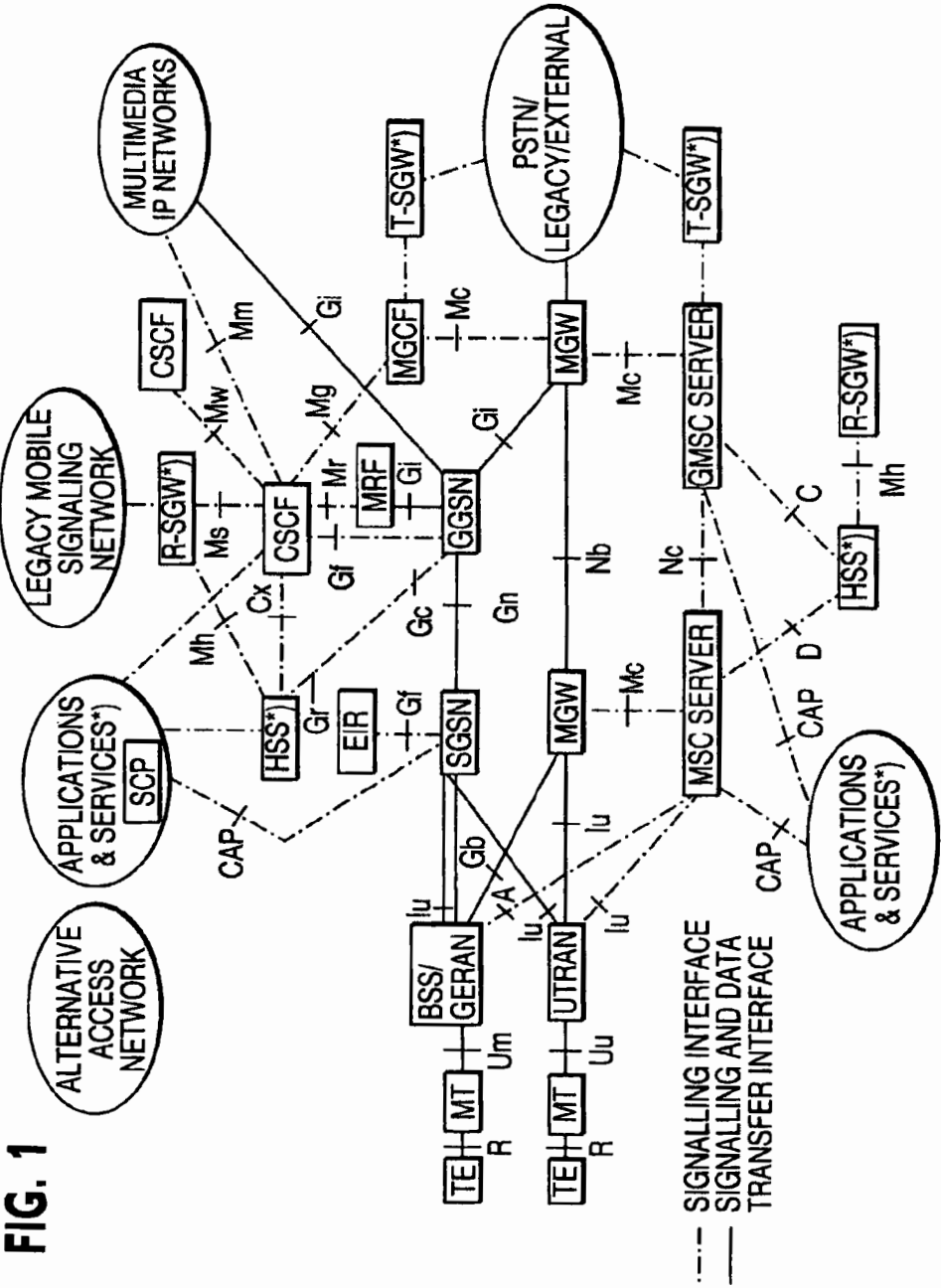


FIG. 2

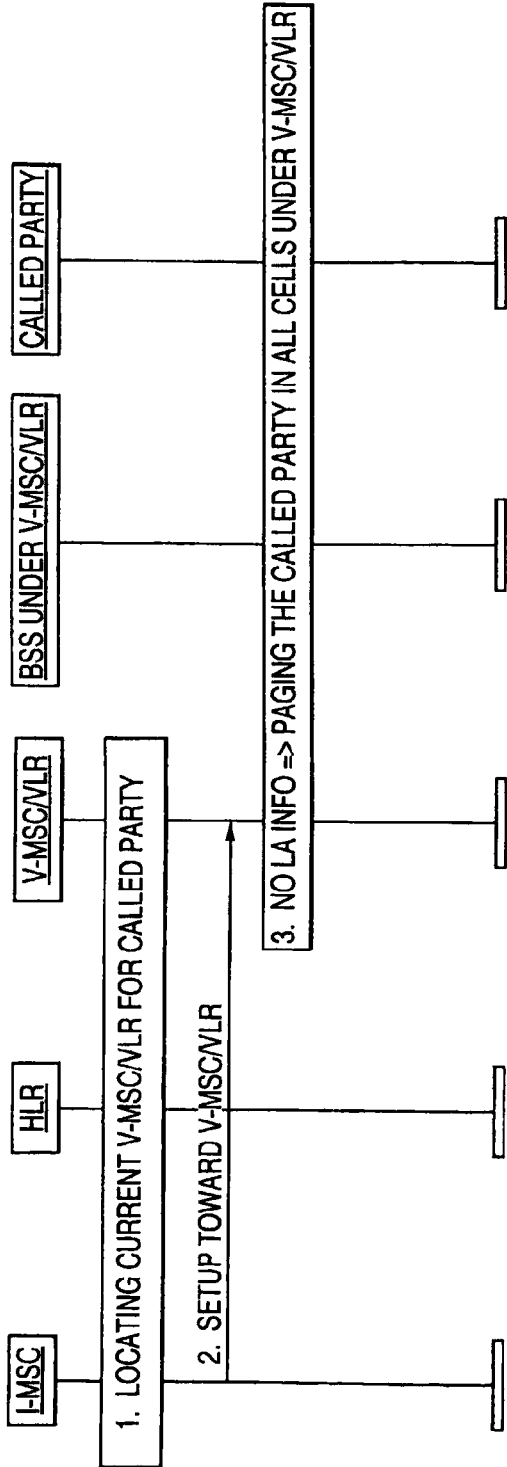
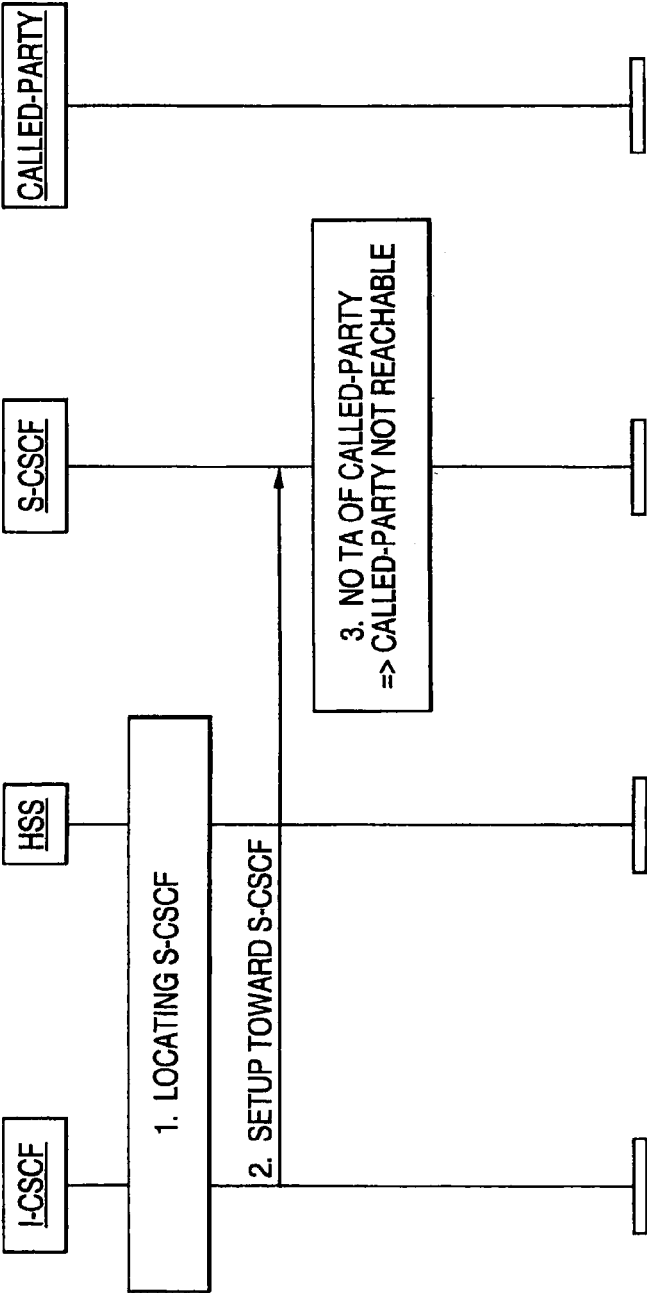


FIG. 3



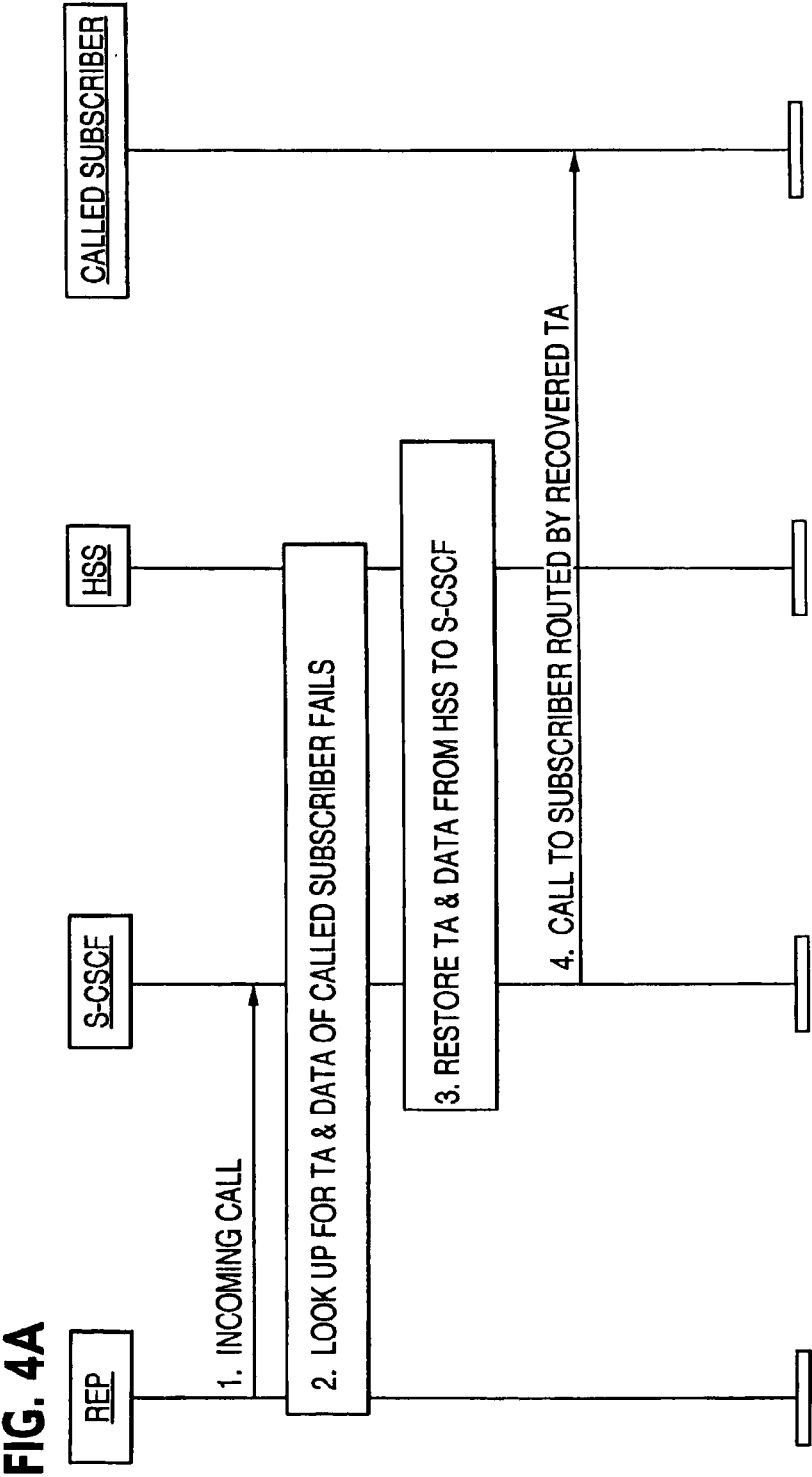
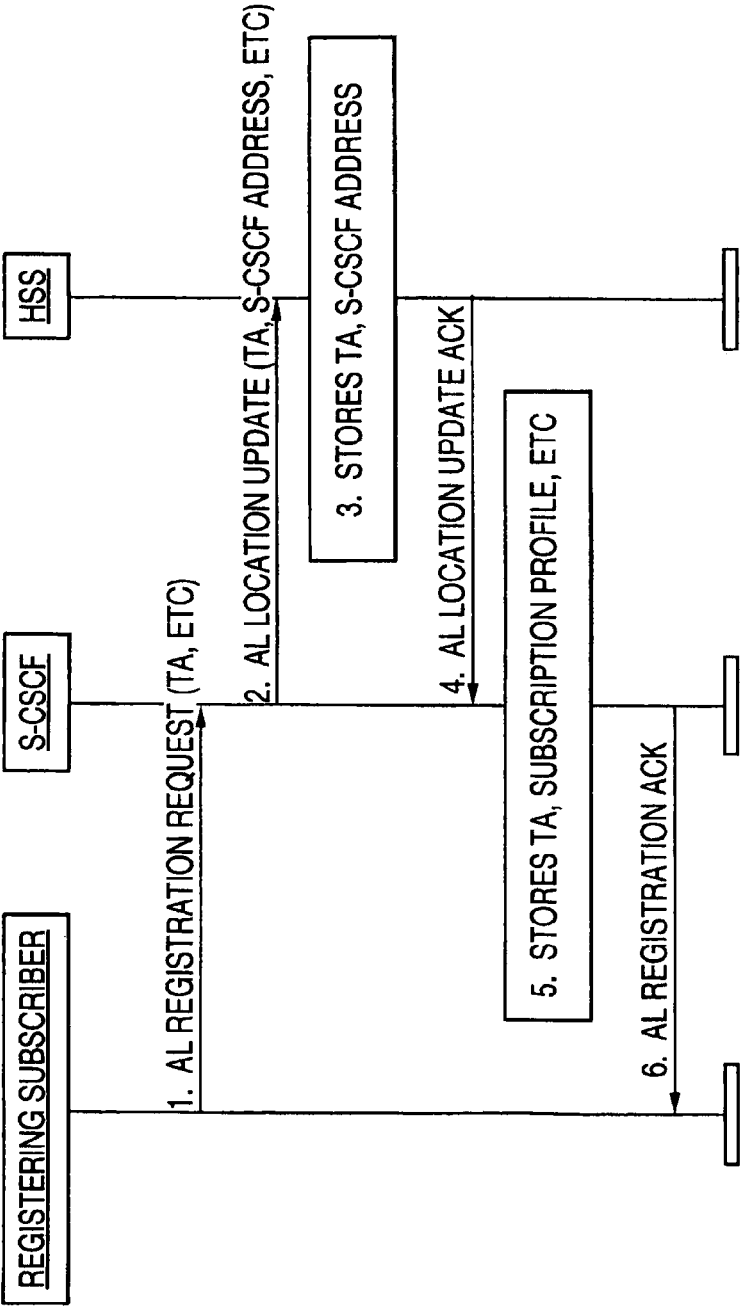
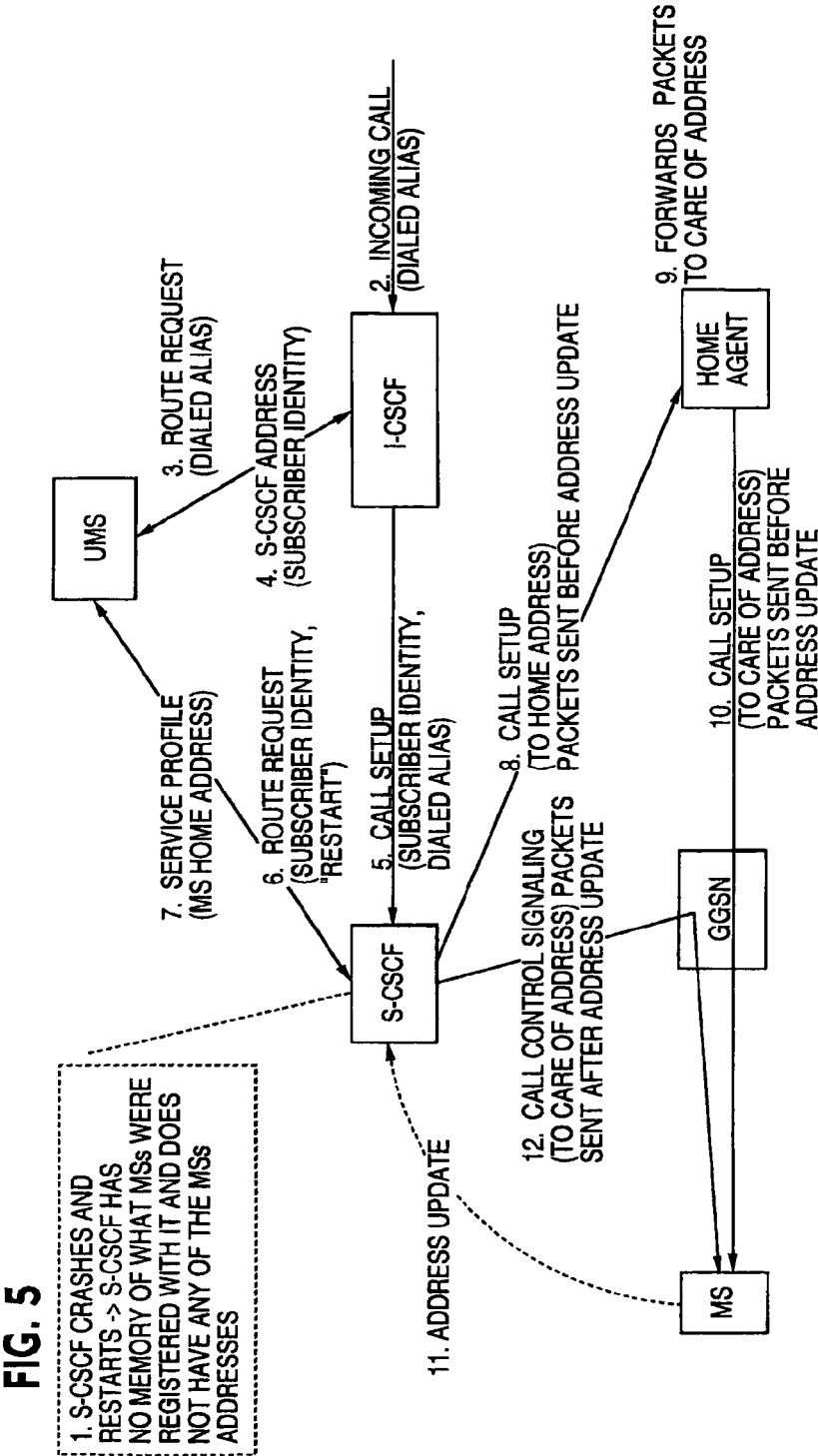


FIG. 4B







US 8,600,372 B2

1

**RECOVERY TECHNIQUES IN MOBILE NETWORKS****CROSS-REFERENCE TO RELATED PATENT APPLICATIONS**

This application is a Continuation of U.S. patent application Ser. No. 13/484,583, filed May 31, 2012, which is a Continuation of U.S. patent application Ser. No. 13/097,709, filed Apr. 29, 2011 (now U.S. Pat. No. 8,200,211), which is a Continuation of U.S. patent application Ser. No. 12/720,862, filed Mar. 10, 2010 (now U.S. Pat. No. 7,937,081), which is a Divisional of U.S. patent application Ser. No. 09/802,861, filed Mar. 12, 2001, (now U.S. Pat. No. 7,769,374), each of which are incorporated herein by reference in their entirety.

**FIELD**

The present disclosure relates to recovery techniques for use in mobile networks. More particularly, the present disclosure relates to protecting the Transport Address (TA) which is a current Care of Address of a mobile subscriber is reachable from loss and after Call State Control Function (CSCF) crashes and after reset situations of a network element realizing CSCF functionality.

**DESCRIPTION OF RELATED ART**

Technical Report TR 23.821 V1.0.1, published July 2000 by the 3rd Generation Partnership Project (3GPP) and available on the Internet at <http://www.3gpp.org>, discloses the specifications of a 3G All-IP mobile network and this report is incorporated by reference herein in its entirety.

FIG. 1 illustrates the architecture of the network disclosed in the above-noted Technical Report. The elements shown with asterisks are elements which have been duplicated for figure layout purposes only. These duplicated elements belong to the same logical element in the reference model.

Unfortunately, the network disclosed in the Technical Report fails to include any protection of the TA of a 3G All-IP subscriber from loss. Furthermore, the network disclosed in the Technical Report fails to protect the IP address of a subscriber in the case of a reset situation of a network element realizing CSCF functionality, that is, a CSCF, thereby preventing recovery after a reset of the network element. Still furthermore, the network disclosed in the Technical Report fails to protect the location information of a subscriber after a CSCF crash, thereby preventing recovery after a CSCF crash.

**SUMMARY**

An object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL (Application Level) location update from the S-CSCF to a Home Subscriber Server (HSS) including the subscriber's TA and the (S-CSCF) address and storing data including the subscriber's TA and the S-CSCF address in the HSS so as to be protected against loss.

Another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL location update from the S-CSCF to an HSS including the S-CSCF address and

2

storing data including the subscriber's TA in a non-volatile memory of the S-CSCF so as to be protected against loss.

Yet another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including upon an S-CSCF receiving a call setup request for the subscriber from an Interrogating Call State Control Function (I-CSCF), forwarding a route request to a User Mobility Server (UMS) and receiving a home address of the subscriber and then forwarding the call setup request from the S-CSCF to a home agent at the home address of the subscriber and then forwarding the call setup request from the home agent to the subscriber and subsequently forwarding an address update from the subscriber to the S-CSCF.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing and a better understanding of the present disclosure will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this disclosure. While the foregoing and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, issued a clearly understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 illustrates the architecture of a 3G All-IP mobile network.

FIG. 2 illustrates reaching a called party after losing LA (Location Area) information in a legacy mobile network.

FIG. 3 illustrates failure to reach a called party after losing TA information in a 3GPP All-IP mobile network.

FIG. 4A illustrates sending subscriber TA to S-CSCF and then forwarding it to HSS at registration.

FIG. 4B illustrates an example of reaching a called party after losing TA information in a mobile network in accordance with the present disclosure.

FIG. 5 illustrates the signal flow in the case of a recovery after a CSCF crash in accordance with another embodiment of the present disclosure.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Before beginning a detailed description of the subject disclosure, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures.

Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, other components may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

In the application level of a 3G All-IP network, the reachability of a subscriber is maintained in two levels, namely, the network element level and the subscriber level. The S-CSCF that the subscriber is currently registered to and the TA of the roaming subscriber, which the subscriber provides to the network during Application Level (AL) registration, must be known to and maintained by the network.

US 8,600,372 B2

3

Without specific support for mobility in IPv6, packets destined to a mobile subscriber would not be able to reach it while the subscriber is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a subscriber could change its IP address each time it moves to a new link, but it would then not be able to maintain transport and higher-layer connections when it changes location.

Mobile IPv6 allows a subscriber to move from one link to another without changing its IP address. A subscriber is always addressable by its "home address", an IP address assigned to it within its home subnet prefix on its home link. Packets may be routed to the subscriber using this address regardless of its current point of attachment to the Internet, and it may continue to communicate with others after moving to a new link. The movement of a subscriber away from its home link is thus transparent to transport and higher-layer protocols and applications.

A mobile subscriber is always addressable by its home address, whether it is currently attached to its home link or is away from home. While it is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if it were never mobile. Since the subnet prefix of its home address is the subnet prefix (or one of the subnet prefixes) on the subscribers' home link (it is the mobile subscribers' home subnet prefix), packets addressed to it will be routed to its home link.

While a subscriber is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while the subscriber is visiting a particular foreign link. The subnet prefix of a subscriber's care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by it; if it is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the subscriber in its location away from home.

The association between a subscriber's home address and care-of address is known as a "binding" for the subscriber. It typically acquires its care-of address through stateless or stateful Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static preassignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this discussion.

While away from home, a mobile subscriber registers one of its care-of addresses with a router on its home link, requesting this router to function as the "home agent" for it. This binding registration is done by the subscriber sending to the home agent a packet containing a "Binding Update" destination option; the home agent then replies to the subscriber by returning a packet containing a "Binding Acknowledgment" destination option. The care-of address in this binding registered with its home agent is known as the subscriber's "primary care-of address". The subscribers' home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the subscribers' home address (or home addresses) on the home link and tunnels each intercepted packet to the subscribers' primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation, with the outer IPv6 header addressed to the subscribers' primary care-of address.

Keeping the address of the S-CSCF ensures that a call to a subscriber can be routed to the destination node, that is, the

4

S-CSCF. Keeping the current TA of the subscriber ensures that a call made to the subscriber which arrives at the S-CSCF can finally reach the subscriber.

As illustrated in FIG. 2, in legacy mobile networks, such as GSM, the information on the serving MSC/VLR (stored in the HLR) is adequate. That is, the called party can be reached even after the loss of the subscriber location area (LA) information by a searching/paging mechanism. In step 1, the current V-MSC/VLR for a called party is first located and in step 2 a setup toward the V-MSC/VLR is performed. In step 3, upon a loss of the LA information, the called party is paged in all cells under the V-MSC/VLR.

On the other hand, as illustrated in FIG. 3, in the 3G All-IP network, no such searching mechanism is available, so that the information of the current S-CSCF (stored in the HSS) is insufficient to reach the subscriber upon the loss of the subscriber TA. In step 1, S-CSCF is located and in step 2 a setup toward the S-CSCF is performed. However, in step 3, in the absence of the TA of the called party, the called party is not reachable.

The applicants have determined that the TA of a 3G All-IP subscriber should be protected against loss with the same level of security as that for the Serving CSCF (S-CSCF). The applicants have proposed options to protect the TA of a subscriber, namely, one option in which the TA is forwarded to the HSS and another option in which there is a security backup of the TA within the CSCF. The TA of the subscriber should be forwarded to the HSS at registration and downloaded from the HSS to the S-CSCF during recovery. Still another option is to have a permanent IPv6 (Internet Protocol Version 6) address allocated to the subscriber and to have the subscriber update its current Care-of Address (part of the TA) to the Home Agent upon obtaining the current TA.

As noted above, in accordance with the present disclosure, various options are available for implementing protection and recovery of the subscriber TA.

In the first option, as illustrated in FIG. 4A, "a safe copy" of the subscriber's TA is forwarded to the HSS for storage and protection. The TA must enjoy the same level of protection against loss as the S-CSCF address. The TA and other data can then be restored to the S-CSCF upon the earlier loss of the data by the S-CSCF. It is noted that the subscriber's TA is stored in the S-CSCF for normal operation. An incoming call from an REP (Remote End-Point) is received by the S-CSCF in step 1. In step 2, the S-CSCF looks for the subscriber's TA so as to route the call but fails to find the subscriber's TA. In step 3, the S-CSCF initiates the restoration of the subscriber's TA (and possibly other data) from the HSS. This option is only available when the S-CSCF loses only the TA of the subscriber. Finally, in step 4, the call is then routed to the subscriber using the recovered TA.

As illustrated in FIG. 4B in step 1, the registering subscriber forwards an AL registration request to the S-CSCF including the TA. In step 2, an AL Location Update is forwarded to the HSS including the TA and S-CSCF address. In step 3, the HSS stores the updated TA and S-CSCF address (in a hard disk, for example, or other non-volatile memory). In step 4, the HSS forwards an AL Location Update acknowledgement to the S-CSCF which stores the TA and subscription profile and other data in step 5. In step 6, the S-CSCF forwards an AL registration acknowledge to the registering subscriber.

In the second option, the same level of protection against loss applies for the subscriber's TA stored in the S-CSCF as that of the S-CSCF address stored in the HSS. For example, the subscriber's TA can be backed up in a hard disk, or other non-volatile memory in the S-CSCF.

US 8,600,372 B2

5

In the case of an S-CSCF crash, when the S-CSCF restarts, all of the information regarding the mobile subscribers registered with it, including the information on how to reach the mobile subscribers, is lost. In such a situation, it is not possible to deliver mobile terminated calls to the mobile subscribers that were registered with the S-CSCF that was restarted.

In providing a solution to the above-noted problem in accordance with the third option, the following assumptions are made:

1) IPv6 is adopted for IP addressing and a subscriber is given a home address at subscription time. This home address is stored in a UMS.

2) The subscriber is in an area assigned to an S-CSCF and has registered with it and has provided its' TA, that is, the current address where the subscriber is reachable. Such an address is not the static home address but rather is the Care-of Address. Whenever the S-CSCF has to forward signaling to the mobile subscriber, it uses the Care-of Address. The subscriber has also registered its current Care of Address with its Home Agent.

3) The S-CSCF restarts due to a fault and loses the information about the mobile station.

The following procedure in accordance with the present disclosure, as illustrated in FIG. 5, may, for example, be used for mobile terminating call delivery when, as illustrated in 1, the S-CSCF crashes and restarts, the S-CSCF has no memory of what mobile stations (MSs) were registered with the S-CSCF and does not have any of the MSs Care of Address addresses:

When an incoming call at 2 reaches a CSCF in the home network, either from another IP based terminal or from an MGCF (Media Gateway Control Function), the I-CSCF queries at 3 the UMS based on the alias dialed by the calling party.

During registration, the UMS has stored information about the S-CSCF and information as to how the mobile subscriber can be reached. More particularly, the UMS has stored the address of the S-CSCF, that is, the address where CC (Call Control) signaling must be forwarded. At this point, two scenarios are possible:

The information in the UMS regarding the S-CSCF is still valid; the UMS returns at 4 the address of the S-CSCF and the Subscriber Identity and then forwards the call setup 5 to the S-CSCF.

The S-CSCF, not having information available for the alias to which the call corresponds due to a crash, queries 6 the UMS based on the Subscriber Identity optionally indicating that a restart took place in order to trigger a profile download.

The UMS returns at 7 the Home Address of the MS to the S-CSCF.

The S-CSCF forwards at 8 the signaling to the Home Address which is the home agent.

The home agent receives the packets at 9 and forwards them at 10 to the MS using the Care of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the MS receives the first packet, it sends at 11 a message to the S-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP) and call control signalling is sent at 12 from the S-CSCF to the MS.

When the call is terminated the subscriber can optionally re-register with the S-CSCF.

2) The information in the UMS is not valid; the UMS returns the Home Address of the mobile subscriber.

The I-CSCF forwards the signaling to the Home Address.

6

The Home Agent receives the packets and forwards them to the Care-of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the mobile subscriber receives the first packet, it sends a message to the I-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP).

When the call is terminated the subscriber can optionally re-register with a S-CSCF.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, drawings, and appended claims without departing from the spirit of the invention. For example, the example embodiments of the present invention have been described with respect to currently used networks, such as 3G All-IP mobile networks, and standards for simplicity. It is, of course, understood that the present invention is not limited thereto. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

1. A method comprising:

receiving at a first server a registration request from a subscriber in a mobile network, wherein the registration request includes a transport address for the subscriber; communicating the transport address and an address of the first server from the first server to a second server for storage;

identifying a loss of the transport address by the first server; and

receiving the stored transport address at the first server from the second server in response to the loss of the transport address by the first server.

2. The method of claim 1, wherein the transport address is stored in a non-volatile memory of the second server.

3. The method of claim 2, wherein the non-volatile memory comprises a hard disk drive.

4. The method of claim 1, wherein the transport address of the subscriber comprises a current care of address of the subscriber.

5. A method of claim 1, wherein the first server is an S-CSCF.

6. The method of claim 1, wherein the second server is an HSS.

7. A non-transitory program storage device readable by a machine, non-transmissible, tangibly embodying a program of instructions executable by the machine to cause the machine to:

receive, at a first server, a registration request from a subscriber in a mobile network, wherein the registration request includes a transport address for the subscriber; communicate the transport address of the subscriber and an address of the first server from the first server to a second server for storage such that the transport address and the address of the first server are stored at the second server; identify a loss of the transport address by the first server; and

7

receive, from the second server, the stored transport address at the first server in response to the loss of the transport address by the first server.

8. The program storage device of claim 7, wherein the transport address and the address of the first server are stored in a non-volatile memory of the second server.

9. The program storage device of claim 8, wherein the non-volatile memory comprises a hard disk drive.

10. The program storage device of claim 7, wherein the first server is an S-CSCF.

11. The program storage device of claim 7, wherein the second server is an HSS.

12. A non-transitory program storage device readable by a machine, non-transmissible, tangibly embodying a program of instructions executable by the machine to cause the machine to:

receive, at a first server, a registration request from a subscriber, wherein the registration request includes a transport address of the subscriber;

store the transport address in a non-volatile memory at the first server;

identify a loss of the transport address by the first server;

restore the transport address to the first server from the non-volatile memory in response to the loss of the transport address by the first server.

8

13. The program storage device of claim 12, wherein the non-volatile memory comprises a hard disk drive.

14. A system comprising:

a receiver at a first server, wherein the receiver is configured to receive a registration request from a subscriber of a mobile network, wherein the registration request includes a transport address of the subscriber;

a transmitter at the first server configured to send the transport address and an address of the first server from the first server to a second server for storage; and

a processor at the first server configured to identify a loss of the transport address by the first server,

wherein the receiver is configured to receive the transport address from the second server in response to the loss of the transport address by the first server.

15. The system of claim 14, further comprising:

a second receiver at the second server, wherein the second receiver is configured to receive from the first server the transport address and the address of the first server, and to receive a request from the first server to restore a stored transport address; and

a second transmitter at the second server, wherein the second transmitter is configured to communicate the transport address to the first server.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 8,600,372 B2  
APPLICATION NO. : 13/682230  
DATED : December 3, 2013  
INVENTOR(S) : Phan-Anh et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page, in Column 1, delete item “(60)” and insert item -- (63) --, therefor.

In the Specifications

In Column 4, Line 10, delete “is.” and insert -- is --, therefor.

In Column 4, Line 19, delete “parry” and insert -- party --, therefor.

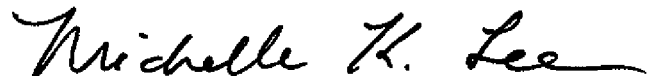
In Column 5, Line 30, delete “addresses:” and insert -- addresses. --, therefor.

In Column 5, Line 65, delete “2)”.

In the Claims

In Column 6, Line 51, in Claim 5, delete “A method” and insert -- The method --, therefor.

Signed and Sealed this  
Twenty-ninth Day of April, 2014



Michelle K. Lee  
*Deputy Director of the United States Patent and Trademark Office*

# Exhibit R

---





US008923846B2

(12) **United States Patent**  
**Phan-Anh et al.**

(10) **Patent No.:** **US 8,923,846 B2**  
(45) **Date of Patent:** **\*Dec. 30, 2014**

(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

(71) Applicant: **Intellectual Ventures I LLC**,  
Wilmington, DE (US)

(72) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Espoo (FI); **Stefano Faccin**, Hayward, CA (US)

(73) Assignee: **Intellectual Ventures I LLC**,  
Wilmington, DE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/058,473**

(22) Filed: **Oct. 21, 2013**

(65) **Prior Publication Data**

US 2014/0045490 A1 Feb. 13, 2014

**Related U.S. Application Data**

(60) Continuation of application No. 13/682,230, filed on Nov. 20, 2012, now Pat. No. 8,600,372, which is a continuation of application No. 13/484,583, filed on May 31, 2012, now Pat. No. 8,351,924, which is a continuation of application No. 13/097,709, filed on Apr. 29, 2011, now Pat. No. 8,200,211, which is a continuation of application No. 12/720,862, filed on Mar. 10, 2010, now Pat. No. 7,937,081, which is a division of application No. 09/802,861, filed on Mar. 12, 2001, now Pat. No. 7,769,374.

(51) **Int. Cl.**  
**H04W 24/00** (2009.01)  
**H04W 24/04** (2009.01)

(52) **U.S. Cl.**  
CPC ..... **H04W 24/04** (2013.01)  
USPC ..... **455/424**; 455/435.1; 455/415; 455/433

(58) **Field of Classification Search**  
CPC ..... H04W 24/00; H04W 24/08  
USPC ..... 455/424, 435.1, 415, 433  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,077,830 A 12/1991 Mallia  
5,274,694 A 12/1993 Lechner et al.

(Continued)

**OTHER PUBLICATIONS**

U.S. Appl. No. 13/682,230, filed Nov. 2012, Phan-Anh et al.\*

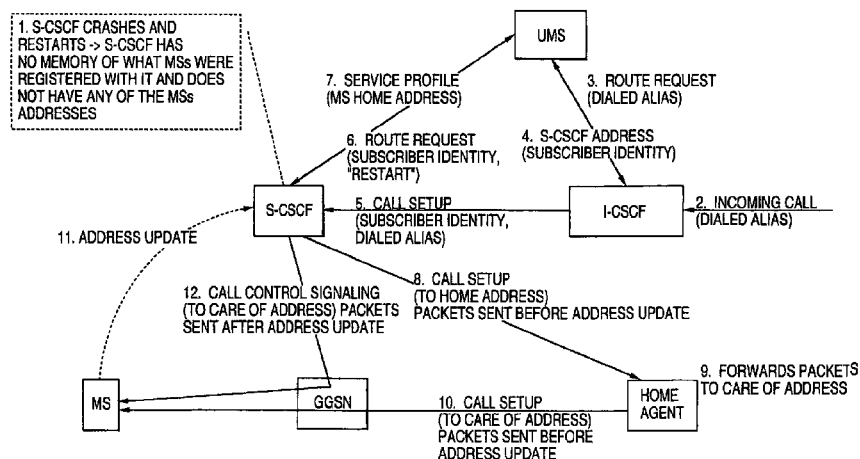
(Continued)

*Primary Examiner* — Nghi H. Ly

(57) **ABSTRACT**

A technique for protecting location information of a subscriber in a mobile network is disclosed. A User Mobility Server (UMS) receives a first query from a first call state control function (CSCF). The UMS transmits a call setup and a subscriber identity to a servicing-call state control function (S-CSCF). The S-CSCF may have no record of the subscriber identity due to a restart or some other event. The UMS receives a second query from the S-CSCF based in part of the subscriber identity. The UMS transmits a home address of a mobile station to the S-CSCF. The UMS may also transmit a profile download to the S-CSCF.

**20 Claims, 6 Drawing Sheets**



**US 8,923,846 B2**

Page 2

(56)

**References Cited****U.S. PATENT DOCUMENTS**

5,463,672	A	10/1995	Kage	
5,561,854	A	10/1996	Antic et al.	
6,097,942	A	8/2000	Laiho	
6,163,532	A	12/2000	Taguchi et al.	
6,408,182	B1	6/2002	Davidson et al.	
6,411,632	B2	6/2002	Lindgren et al.	
6,445,911	B1	9/2002	Chow et al.	
6,587,882	B1	7/2003	Inoue et al.	
6,594,490	B1	7/2003	Toyoda et al.	
6,600,920	B1	7/2003	Stephens et al.	
6,636,491	B1	10/2003	Kari et al.	
6,654,606	B1	11/2003	Foti et al.	
6,707,813	B1	3/2004	Hasan et al.	
6,721,291	B1	4/2004	Bergenwall et al.	
6,732,177	B1	5/2004	Roy	
6,763,233	B2	7/2004	Bharatia	
6,775,255	B1	8/2004	Roy	
6,839,323	B1	1/2005	Foti	
7,006,449	B2	2/2006	Teraoka	
7,092,390	B2 *	8/2006	Wan	370/392
7,221,940	B2	5/2007	Kaneko et al.	
7,602,762	B1	10/2009	Kauppinen et al.	
7,769,374	B2 *	8/2010	Phan-Anh et al.	455/424
7,937,081	B2	5/2011	Phan-Anh et al.	
8,200,211	B2	6/2012	Phan-Anh et al.	
8,514,808	B2 *	8/2013	Cheng et al.	370/331
8,554,231	B2 *	10/2013	Jones	455/439
2001/0031635	A1	10/2001	Bharatia	
2002/0147845	A1	10/2002	Sanchez-Herrero et al.	
2009/0029701	A1	1/2009	Mishima	
2011/0076991	A1	3/2011	Mueck et al.	

**OTHER PUBLICATIONS**

International Preliminary Examination Report for PCT/IB02/00721 completed Apr. 3, 2003.

International Search Report for PCT/IB02/00721, mailed Feb. 26, 2003.  
 Technical Report TR 23.821 V1.0.1, published Jul. 2000 by the 3<sup>rd</sup> Generation partnership Project 3GPP. 1-62 pages.  
 Notice of Allowance on U.S. Appl. No. 12/720,862, mailed Dec. 27, 2010.  
 Non-Final Office Action on U.S. Appl. No. 12/720,862, mailed Jul. 8, 2010.  
 Notice of Allowance on U.S. Appl. No. 09/802,861 mailed Nov. 25, 2009.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Aug. 3, 2009.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Sep. 23, 2008.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Apr. 8, 2008.  
 Re-Exam 95/001,899, filed May 31, 2012, Son Phan-Anh, et al.  
 Re-Exam 95/002,004, filed Aug. 6, 2012, Son Phan-Anh, et al.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Oct. 11, 2007.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed May 8, 2007.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Jun. 30, 2006.  
 Final Office Action on U.S. Appl. No. 09/802,861 mailed Apr. 6, 2005.  
 Non-final Office Action on U.S. Appl. No. 09/802,861 mailed Nov. 28, 2003.  
 Notice of Allowance on U.S. Appl. No. 12/720,862 mailed Dec. 27, 2010.  
 Non-final Office Action on U.S. Appl. No. 12/720,862 mailed Jul. 8, 2010.  
 Notice of Allowance on U.S. Appl. No. 13/097,709 mailed Feb. 22, 2012.  
 Non-final Office Action on U.S. Appl. No. 13/097,709 mailed Sep. 1, 2011.  
 Notice of Allowance on U.S. Appl. 13/484,583, mailed Sep. 12, 2012.

\* cited by examiner

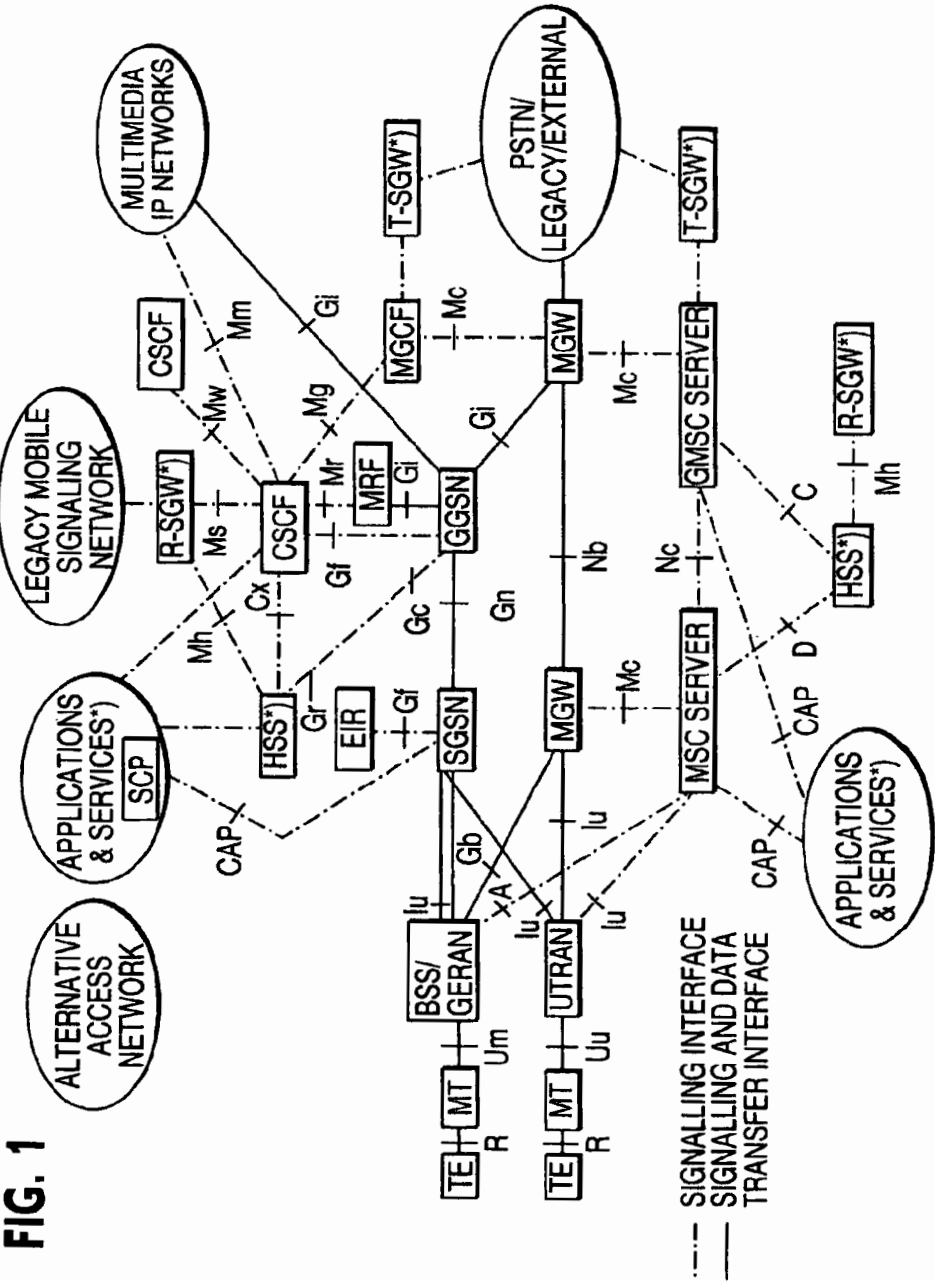


FIG. 2

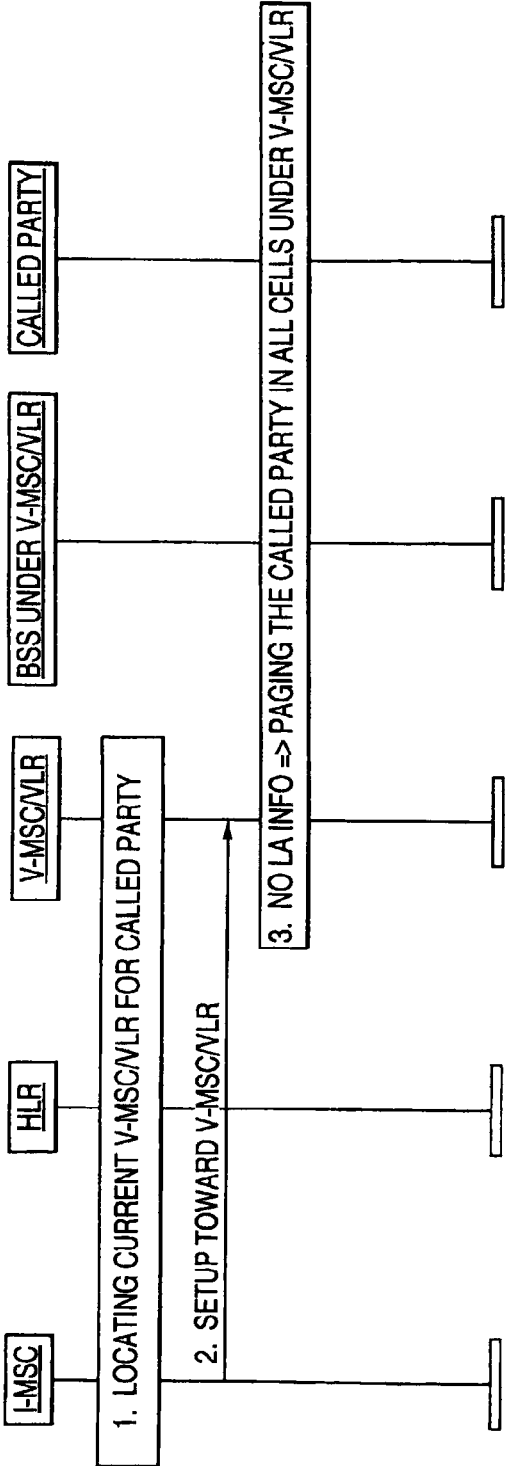


FIG. 3

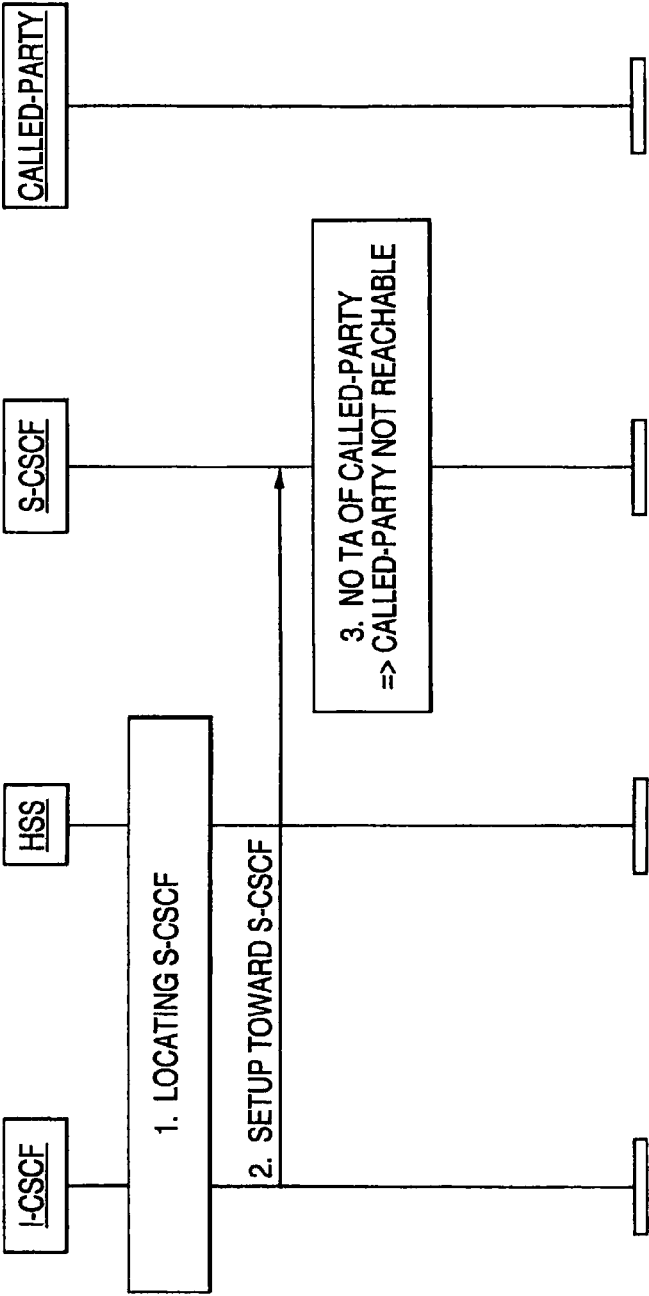


FIG. 4A

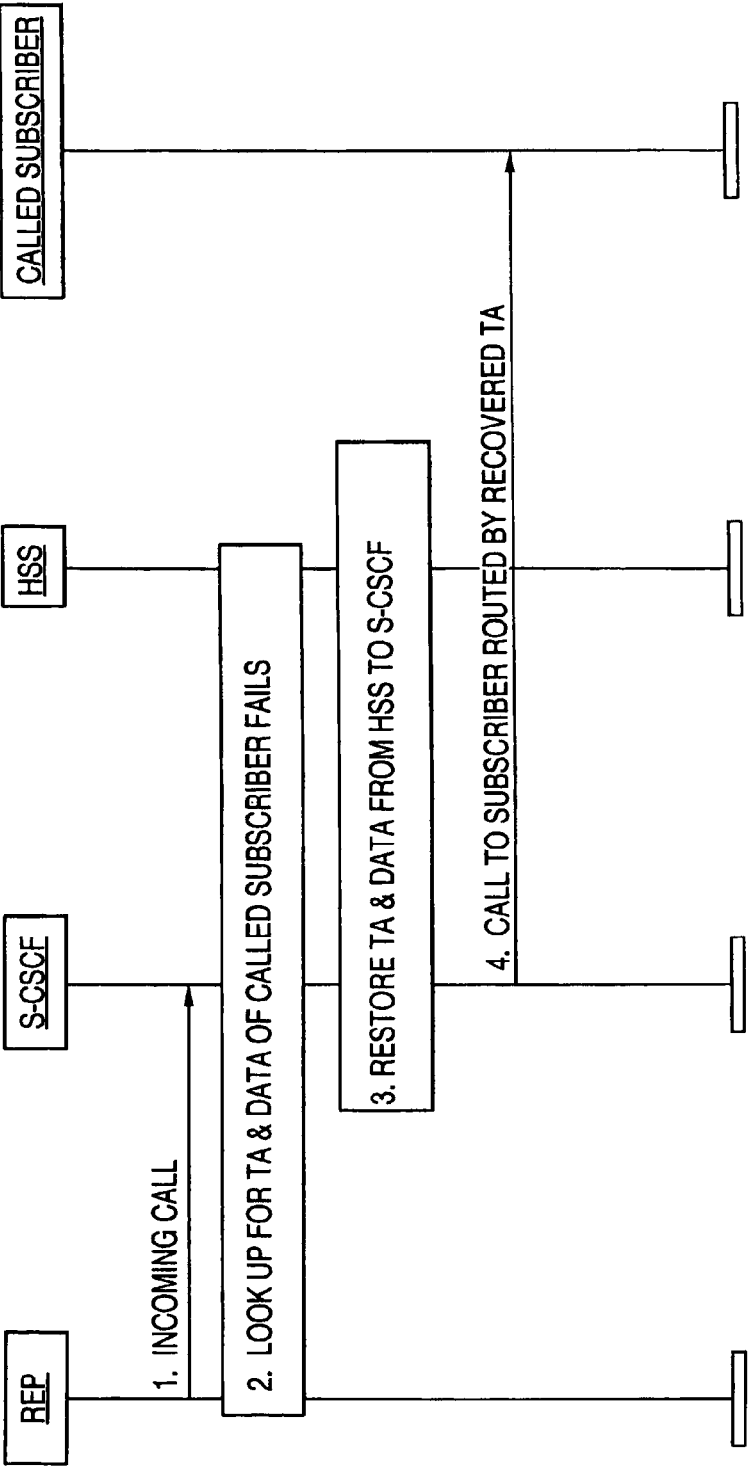
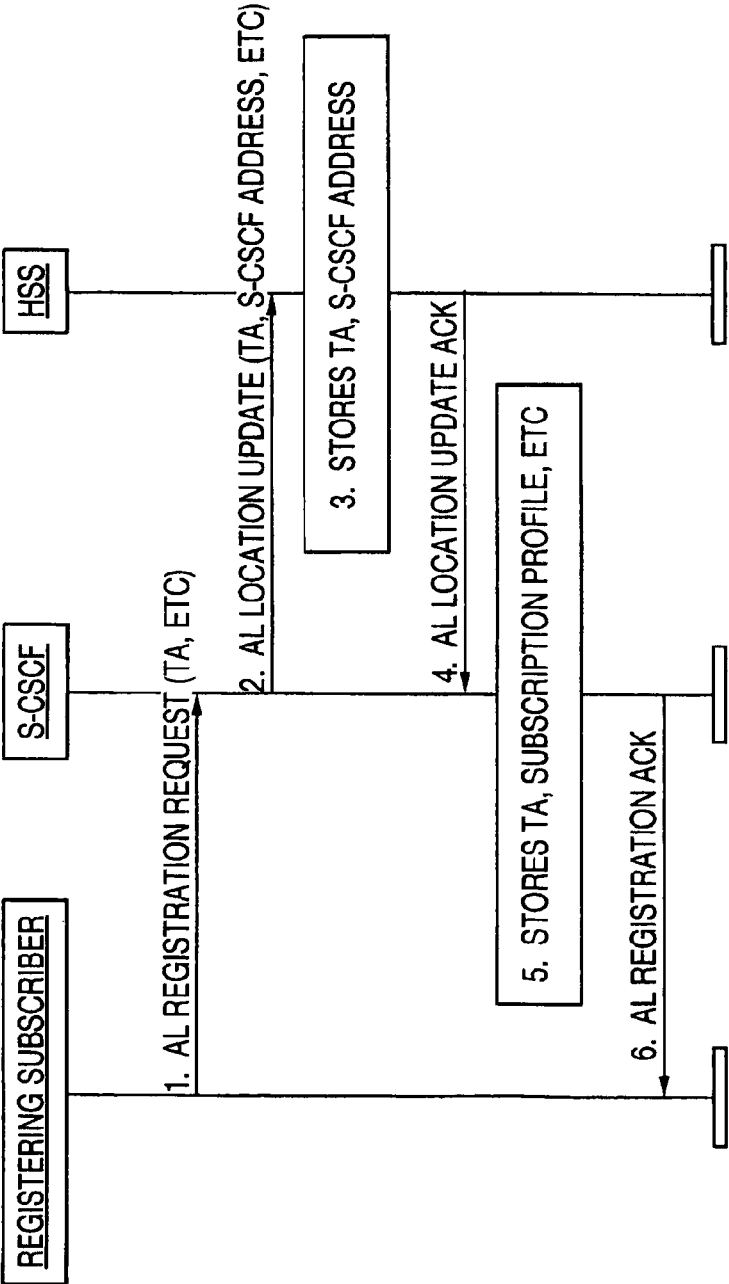
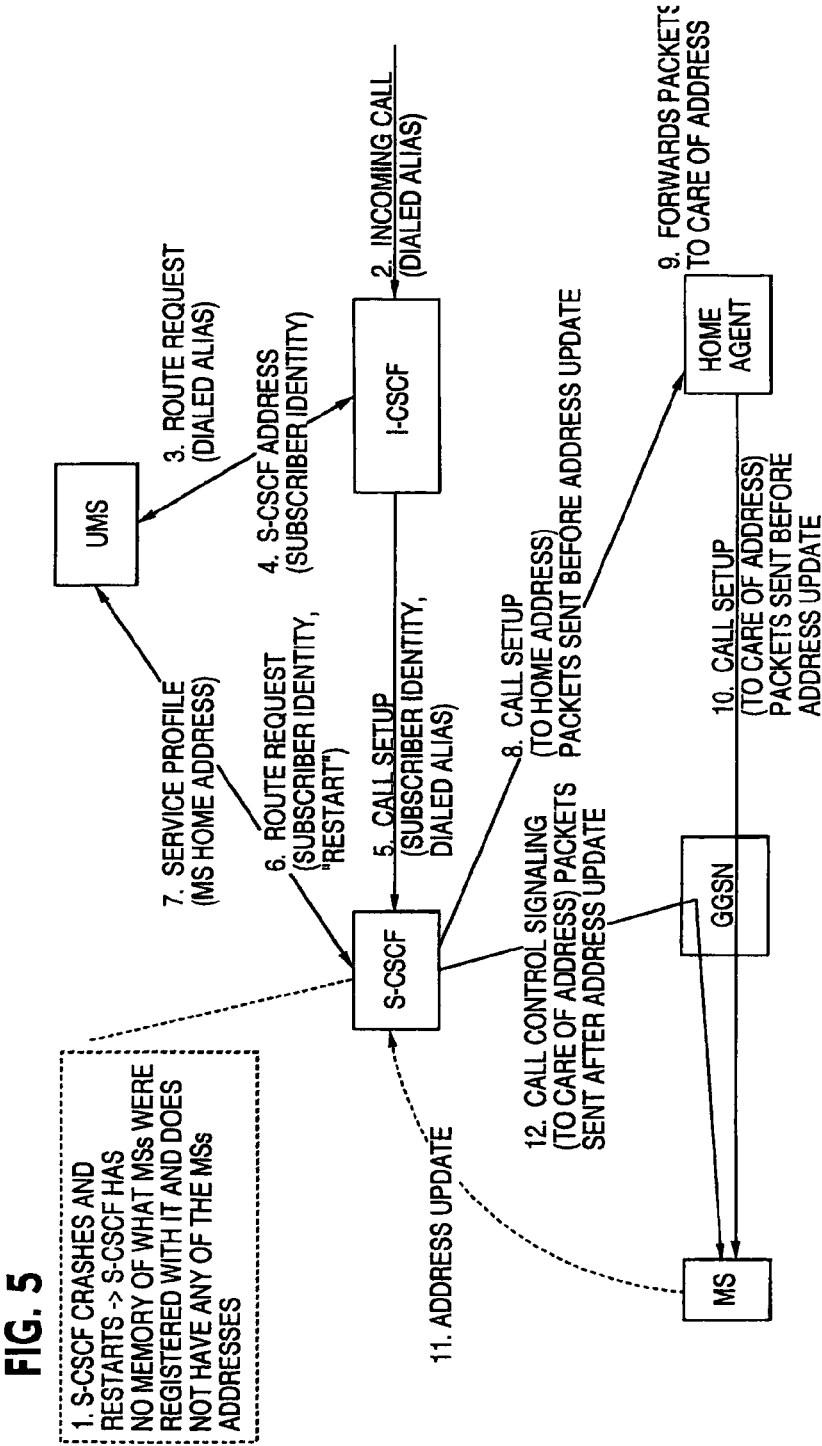


FIG. 4B







US 8,923,846 B2

1

**RECOVERY TECHNIQUES IN MOBILE NETWORKS****CROSS-REFERENCE TO RELATED PATENT APPLICATIONS**

This application is a Continuation of U.S. application Ser. No. 13/682,230, filed Nov. 20, 2012, which is a Continuation of U.S. application Ser. No. 13/484,583, filed May 31, 2012 (now U.S. Pat. No. 8,351,924), which is a Continuation of U.S. application Ser. No. 13/097,709, filed Apr. 29, 2011 (now U.S. Pat. No. 8,200,211, which is a Continuation of U.S. application Ser. No. 12/720,862, filed Mar. 10, 2010 (now U.S. Pat. No. 7,937,081, which is a Divisional of U.S. application Ser. No. 09/802,861, filed Mar. 12, 2001, (now U.S. Pat. No. 7,769,374) all of which are incorporated herein by reference in their entirety.

**FIELD**

The present disclosure relates to recovery techniques for use in mobile networks. More particularly, the present disclosure relates to protecting the Transport Address (TA) which is a current Care of Address of a mobile subscriber is reachable from loss and after Call State Control Function (CSCF) crashes and after reset situations of a network element realizing CSCF functionality.

**DESCRIPTION OF RELATED ART**

Technical Report TR 23.821 V1.0.1, published July 2000 by the 3rd Generation Partnership Project (3GPP) and available on the Internet at <http://www.3gpp.org>, discloses the specifications of a 3G All-IP mobile network and this report is incorporated by reference herein in its entirety.

FIG. 1 illustrates the architecture of the network disclosed in the above-noted Technical Report. The elements shown with asterisks are elements which have been duplicated for figure layout purposes only. These duplicated elements belong to the same logical element in the reference model.

Unfortunately, the network disclosed in the Technical Report fails to include any protection of the TA of a 3G All-IP subscriber from loss. Furthermore, the network disclosed in the Technical Report fails to protect the IP address of a subscriber in the case of a reset situation of a network element realizing CSCF functionality, that is, a CSCF, thereby preventing recovery after a reset of the network element. Still furthermore, the network disclosed in the Technical Report fails to protect the location information of a subscriber after a CSCF crash, thereby preventing recovery after a CSCF crash.

**SUMMARY**

An object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL (Application Level) location update from the S-CSCF to a Home Subscriber Server (HSS) including the subscriber's TA and the (S-CSCF) address and storing data including the subscriber's TA and the S-CSCF address in the HSS so as to be protected against loss.

Another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL location update from

2

the S-CSCF to an HSS including the S-CSCF address and storing data including the subscriber's TA in a non-volatile memory of the S-CSCF so as to be protected against loss.

Yet another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including upon an S-CSCF receiving a call setup request for the subscriber from an Interrogating Call State Control Function (I-CSCF), forwarding a route request to a User Mobility Server (UMS) and receiving a home address of the subscriber and then forwarding the call setup request from the S-CSCF to a home agent at the home address of the subscriber and then forwarding the call setup request from the home agent to the subscriber and subsequently forwarding an address update from the subscriber to the S-CSCF.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing and a better understanding of the present disclosure will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this disclosure. While the foregoing and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, issued a clearly understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 illustrates the architecture of a 3G All-IP mobile network.

FIG. 2 illustrates reaching a called party after losing LA (Location Area) information in a legacy mobile network.

FIG. 3 illustrates failure to reach a called party after losing TA information in a 3GPP All-IP mobile network.

FIG. 4A illustrates sending subscriber TA to S-CSCF and then forwarding it to HSS at registration.

FIG. 4B illustrates an example of reaching a called party after losing TA information in a mobile network in accordance with the present disclosure.

FIG. 5 illustrates the signal flow in the case of a recovery after a CSCF crash in accordance with another embodiment of the present disclosure.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Before beginning a detailed description of the subject disclosure, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, other components may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

In the application level of a 3G All-IP network, the reachability of a subscriber is maintained in two levels, namely, the network element level and the subscriber level. The S-CSCF that the subscriber is currently registered to and the TA of the roaming subscriber, which the subscriber provides to the network during Application Level (AL) registration, must be known to and maintained by the network.

US 8,923,846 B2

3

Without specific support for mobility in IPv6, packets destined to a mobile subscriber would not be able to reach it while the subscriber is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a subscriber could change its IP address each time it moves to a new link, but it would then not be able to maintain transport and higher-layer connections when it changes location.

Mobile IPv6 allows a subscriber to move from one link to another without changing its IP address. A subscriber is always addressable by its "home address", an IP address assigned to it within its home subnet prefix on its home link. Packets may be routed to the subscriber using this address regardless of its current point of attachment to the Internet, and it may continue to communicate with others after moving to a new link. The movement of a subscriber away from its home link is thus transparent to transport and higher-layer protocols and applications.

A mobile subscriber is always addressable by its home address, whether it is currently attached to its home link or is away from home. While it is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if it were never mobile. Since the subnet prefix of its home address is the subnet prefix (or one of the subnet prefixes) on the subscribers' home link (it is the mobile subscribers' home subnet prefix), packets addressed to it will be routed to its home link.

While a subscriber is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while the subscriber is visiting a particular foreign link. The subnet prefix of a subscriber's care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by it; if it is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the subscriber in its location away from home.

The association between a subscriber's home address and care-of address is known as a "binding" for the subscriber. It typically acquires its care-of address through stateless or stateful Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static preassignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this discussion.

While away from home, a mobile subscriber registers one of its care-of addresses with a router on its home link, requesting this router to function as the "home agent" for it. This binding registration is done by the subscriber sending to the home agent a packet containing a "Binding Update" destination option; the home agent then replies to the subscriber by returning a packet containing a "Binding Acknowledgment" destination option. The care-of address in this binding registered with its home agent is known as the subscriber's "primary care-of address". The subscribers' home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the subscribers' home address (or home addresses) on the home link and tunnels each intercepted packet to the subscribers' primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation, with the outer IPv6 header addressed to the subscribers' primary care-of address.

Keeping the address of the S-CSCF ensures that a call to a subscriber can be routed to the destination node, that is, the

4

S-CSCF. Keeping the current TA of the subscriber ensures that a call made to the subscriber which arrives at the S-CSCF can finally reach the subscriber.

As illustrated in FIG. 2, in legacy mobile networks, such as GSM, the information on the serving MSC/VLR (stored in the HLR) is adequate. That is, the called party can be reached even after the loss of the subscriber location area (LA) information by a searching/paging mechanism. In step 1, the current V-MSC/VLR for a called party is first located and in step 2 a setup toward the V-MSC/VLR is performed. In step 3, upon a loss of the LA information, the called party is paged in all cells under the V-MSC/VLR.

On the other hand, as illustrated in FIG. 3, in the 3G All-IP network, no such searching mechanism is available, so that the information of the current S-CSCF (stored in the HSS) is insufficient to reach the subscriber upon the loss of the subscriber TA. In step 1, S-CSCF is located and in step 2 a setup toward the S-CSCF is performed. However, in step 3, in the absence of the TA of the called party, the called party is not reachable.

The applicants have determined that the TA of a 3G All-IP subscriber should be protected against loss with the same level of security as that for the Serving CSCF (S-CSCF). The applicants have proposed options to protect the TA of a subscriber, namely, one option in which the TA is forwarded to the HSS and another option in which there is a security backup of the TA within the CSCF. The TA of the subscriber should be forwarded to the HSS at registration and downloaded from the HSS to the S-CSCF during recovery. Still another option is to have a permanent IPv6 (Internet Protocol Version 6) address allocated to the subscriber and to have the subscriber update its current Care-of Address (part of the TA) to the Home Agent upon obtaining the current TA.

As noted above, in accordance with the present disclosure, various options are available for implementing protection and recovery of the subscriber TA.

In the first option, as illustrated in FIG. 4A, "a safe copy" of the subscriber's TA is forwarded to the HSS for storage and protection. The TA must enjoy the same level of protection against loss as the S-CSCF address. The TA and other data can then be restored to the S-CSCF upon the earlier loss of the data by the S-CSCF. It is noted that the subscriber's TA is stored in the S-CSCF for normal operation. An incoming call from an REP (Remote End-Point) is received by the S-CSCF in step 1. In step 2, the S-CSCF looks for the subscriber's TA so as to route the call but fails to find the subscriber's TA. In step 3, the S-CSCF initiates the restoration of the subscriber's TA (and possibly other data) from the HSS. This option is only available when the S-CSCF loses only the TA of the subscriber. Finally, in step 4, the call is then routed to the subscriber using the recovered TA.

As illustrated in FIG. 4B in step 1, the registering subscriber forwards an AL registration request to the S-CSCF including the TA. In step 2, an AL Location Update is forwarded to the HSS including the TA and S-CSCF address. In step 3, the HSS stores the updated TA and S-CSCF address (in a hard disk, for example, or other non-volatile memory). In step 4, the HSS forwards an AL Location Update acknowledgement to the S-CSCF which stores the TA and subscription profile and other data in step 5. In step 6, the S-CSCF forwards an AL registration acknowledge to the registering subscriber.

In the second option, the same level of protection against loss applies for the subscriber's TA stored in the S-CSCF as that of the S-CSCF address stored in the HSS. For example, the subscriber's TA can be backed up in a hard disk, or other non-volatile memory in the S-CSCF.

US 8,923,846 B2

5

In the case of an S-CSCF crash, when the S-CSCF restarts, all of the information regarding the mobile subscribers registered with it, including the information on how to reach the mobile subscribers, is lost. In such a situation, it is not possible to deliver mobile terminated calls to the mobile subscribers that were registered with the S-CSCF that was restarted.

In providing a solution to the above-noted problem in accordance with the third option, the following assumptions are made:

1) IPv6 is adopted for IP addressing and a subscriber is given a home address at subscription time. This home address is stored in a UMS.

2) The subscriber is in an area assigned to an S-CSCF and has registered with it and has provided its' TA, that is, the current address where the subscriber is reachable. Such an address is not the static home address but rather is the Care-of Address. Whenever the S-CSCF has to forward signaling to the mobile subscriber, it uses the Care-of Address. The subscriber has also registered its current Care of Address with its Home Agent.

3) The S-CSCF restarts due to a fault and loses the information about the mobile station.

The following procedure in accordance with the present disclosure, as illustrated in FIG. 5, may, for example, be used for mobile terminating call delivery when, as illustrated in 1, the S-CSCF crashes and restarts, the S-CSCF has no memory of what mobile stations (MSs) were registered with the S-CSCF and does not have any of the MSs Care of Address addresses:

When an incoming call at 2 reaches a CSCF in the home network, either from another IP based terminal or from an MGCF (Media Gateway Control Function), the I-CSCF queries at 3 the UMS based on the alias dialed by the calling party.

During registration, the UMS has stored information about the S-CSCF and information as to how the mobile subscriber can be reached. More particularly, the UMS has stored the address of the S-CSCF, that is, the address where CC (Call Control) signaling must be forwarded. At this point, two scenarios are possible:

The information in the UMS regarding the S-CSCF is still valid; the UMS returns at 4 the address of the S-CSCF and the Subscriber Identity and then forwards the call setup 5 to the S-CSCF.

The S-CSCF, not having information available for the alias to which the call corresponds due to a crash, queries 6 the UMS based on the Subscriber Identity optionally indicating that a restart took place in order to trigger a profile download.

The UMS returns at 7 the Home Address of the MS to the S-CSCF.

The S-CSCF forwards at 8 the signaling to the Home Address which is the home agent.

The home agent receives the packets at 9 and forwards them at 10 to the MS using the Care of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the MS receives the first packet, it sends at 11 a message to the S-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP) and call control signalling is sent at 12 from the S-CSCF to the MS.

When the call is terminated the subscriber can optionally re-register with the S-CSCF.

2) The information in the UMS is not valid; the UMS returns the Home Address of the mobile subscriber.

The I-CSCF forwards the signaling to the Home Address.

6

The Home Agent receives the packets and forwards them to the Care-of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the mobile subscriber receives the first packet, it sends a message to the I-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP).

When the call is terminated the subscriber can optionally re-register with a S-CSCF.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, drawings, and appended claims without departing from the spirit of the invention. For example, the example embodiments of the present invention have been described with respect to currently used networks, such as 313 All-IP mobile networks, and standards for simplicity. It is, of course, understood that the present invention is not limited thereto. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

1. A method comprising:

receiving, from a first server at a second server, a transport address and an address of the first server;

receiving, at the second server, a request from the first server to restore the transport address; and

in response to the request from the first server to restore the transport address, communicating the transport address to the first server from the second server.

2. The method of claim 1, wherein the second server is a home subscription server (HSS).

3. The method of claim 1, wherein the first server is a serving-call state control function (S-CSCF).

4. The method of claim 1, further comprising storing the transport address at the second server.

5. The method of claim 4, wherein the storing the transport address comprises storing the transport address in a non-volatile memory of the second server.

6. The method of claim 1, wherein the transport address comprises a care-of-address of a mobile subscriber.

7. The method of claim 1, wherein the receiving, at the second server, the request from the first server to restore the transport address is in response to a loss of the transport address by the first server.

8. The method of claim 1, wherein the receiving the transport address and an address of the first server comprises receiving an application level update message at the second server from the first server.

9. An apparatus comprising:

a receiver configured to receive a transport address and an address of a first server from the first server, wherein the receiver is further configured to receive a request to restore the transport address from the first server; and

a transmitter configured to communicate the transport address to the first server in response to the request to restore the transport address from the first server.

10. The apparatus of claim 9, wherein the apparatus is an HSS.

US 8,923,846 B2

7

11. The apparatus of claim 9, wherein the first server is an S-CSCF.
12. The apparatus of claim 9, further comprising a non-volatile memory configured to store the transport address at the second server.
13. The apparatus of claim 9, wherein the transport address comprises a care-of-address of a mobile subscriber.
14. The apparatus of claim 9, wherein the receiver is further configured to receive the request from the first server to restore the transport address in response to a loss of the transport address by the first server.
15. The apparatus of claim 9, wherein the receiver is further configured to receive the transport address and an address of the first server in an application level update message from the first server.
16. A non-transitory computer-readable medium having instructions stored thereon that, upon execution by a computing device, cause the computing device to perform operations comprising:

8

- receiving, from a first server, a transport address and an address of the first server;
- receiving a request from the first server to restore the transport address; and
- in response to the request from the first server to restore the transport address, communicating the transport address to the first server.
17. The non-transitory computer-readable medium of claim 16, wherein the computing device is an HSS.
18. The non-transitory computer-readable medium of claim 16, wherein the first server is an S-CSCF.
19. The non-transitory computer-readable medium of claim 16, wherein the operations further comprise storing the transport address in a non-volatile memory.
20. The non-transitory computer-readable medium of claim 16, wherein the transport address comprises a care-of-address of a mobile subscriber.

\* \* \* \* \*

# Exhibit S

---





US009918222B2

(12) **United States Patent**  
**Phan-Anh et al.**

(10) **Patent No.:** **US 9,918,222 B2**

(45) **Date of Patent:** **Mar. 13, 2018**

(54) **RECOVERY TECHNIQUES IN MOBILE NETWORKS**

*H04W 24/04* (2009.01)

*H04W 24/02* (2009.01)

*H04W 8/30* (2009.01)

(71) Applicant: **Intellectual Ventures I LLC**,  
Wilmington (DE)

(52) **U.S. Cl.**

CPC ..... *H04W 8/26* (2013.01); *H04W 8/30*  
(2013.01); *H04W 24/02* (2013.01); *H04W*  
*24/04* (2013.01)

(72) Inventors: **Son Phan-Anh**, Budapest (HU); **Balint Benko**, Budapest (HU); **Auvo Hartikainen**, Budapest (HU); **Markku Verkama**, Espoo (FI); **Heikki Juhani Einola**, Espoo (FI); **Stefano Faccin**, Hayward, CA (US)

(58) **Field of Classification Search**

CPC ..... *H04W 8/26*; *H04W 8/30*; *H04W 24/02*  
USPC ..... 455/445, 414.1, 415, 417  
See application file for complete search history.

(73) Assignee: **Intellectual Ventures I LLC**,  
Wilmington, DE (US)

(56)

**References Cited**

U.S. PATENT DOCUMENTS

5,077,830 A 12/1991 Mallia  
5,274,694 A 12/1993 Lechner et al.  
(Continued)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/226,422**

(22) Filed: **Aug. 2, 2016**

OTHER PUBLICATIONS

Final Office Action on U.S. Appl. No. 14/058,473, dated Jun. 6, 2014.

(65) **Prior Publication Data**

US 2017/0078871 A1 Mar. 16, 2017

(Continued)

**Related U.S. Application Data**

(60) Continuation of application No. 14/549,714, filed on Nov. 21, 2014, now Pat. No. 9,432,842, which is a continuation of application No. 14/058,473, filed on Oct. 21, 2013, now Pat. No. 8,923,846, which is a continuation of application No. 13/682,230, filed on Nov. 20, 2012, now Pat. No. 8,600,372, which is a continuation of application No. 13/484,583, filed on May 31, 2012, now Pat. No. 8,351,924, which is a continuation of application No. 13/097,709, filed on Apr. 29, 2011, now Pat. No. 8,200,211, which is a  
(Continued)

Primary Examiner — Nghi H Ly

(57)

**ABSTRACT**

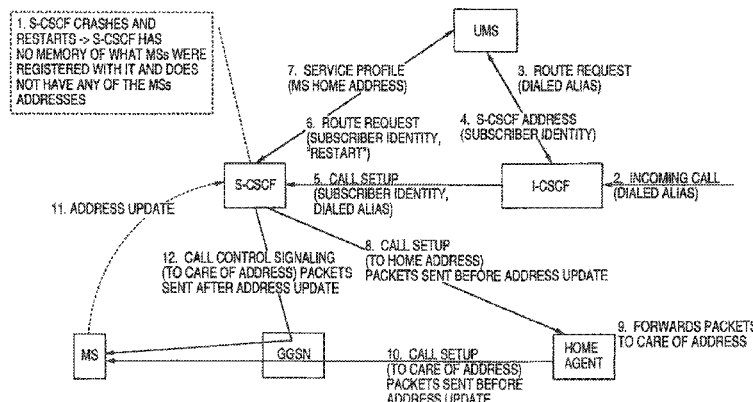
A technique for protecting location information of a subscriber in a mobile network is disclosed. A User Mobility Server (UMS) receives a first query from a first call state control function (CSCF). The UMS transmits a call setup and a subscriber identity to a servicing-call state control function (S-CSCF). The S-CSCF may have no record of the subscriber identity due to a restart are some other event. The UMS receives a second query from the S-CSCF based in part of the subscriber identity. The UMS transmits a home address of a mobile station to the S-CSCF. The UMS may also transmit a profile download to the S-CSCF.

**18 Claims, 6 Drawing Sheets**

(51) **Int. Cl.**

*H04W 40/00* (2009.01)

*H04W 8/26* (2009.01)





**US 9,918,222 B2**

Page 2

**Related U.S. Application Data**

continuation-in-part of application No. 12/720,862, filed on Mar. 10, 2010, now Pat. No. 7,937,081, which is a division of application No. 09/082,861, filed on Mar. 12, 2001, now Pat. No. 7,769,374.

8,600,372	B2	12/2013	Phan-Anh et al.	
8,923,846	B2	12/2014	Phan-Anh et al.	
2004/0121775	A1 *	6/2004	Ropolyi .....	H04L 63/00 455/445
2009/0029701	A1	1/2009	Mishima	
2011/0076991	A1	3/2011	Mueck et al.	
2011/0319089	A1 *	12/2011	Sharma .....	H04W 76/026 455/445

(56)

**References Cited****U.S. PATENT DOCUMENTS**

5,463,672	A	10/1995	Kage	
5,561,854	A	10/1996	Antic et al.	
6,097,942	A	8/2000	Laiho	
6,163,532	A	12/2000	Taguchi et al.	
6,374,302	B1	4/2002	Galasso et al.	
6,408,182	B1	6/2002	Davidson et al.	
6,411,632	B2	6/2002	Lindgren et al.	
6,445,911	B1	9/2002	Chow et al.	
6,584,098	B1	6/2003	Dutnall	
6,587,882	B1	7/2003	Inoue et al.	
6,594,490	B1	7/2003	Toyoda et al.	
6,600,920	B1	7/2003	Stephens et al.	
6,636,491	B1	10/2003	Kari et al.	
6,654,606	B1	11/2003	Foti et al.	
6,707,813	B1	3/2004	Hasan et al.	
6,721,291	B1	4/2004	Bergenwall et al.	
6,732,177	B1	5/2004	Roy	
6,763,233	B2	7/2004	Bharatia	
6,775,255	B1	8/2004	Roy	
6,839,323	B1	1/2005	Foti	
6,859,448	B1	2/2005	Roy	
7,006,449	B2	2/2006	Teraoka	
7,092,390	B2	8/2006	Wan	
7,221,940	B2	5/2007	Kaneko et al.	
7,602,762	B1 *	10/2009	Kauppinen .....	H04L 29/06027 370/349
7,769,374	B2	8/2010	Phan-Anh et al.	
7,937,081	B2	5/2011	Phan-Anh et al.	
8,514,808	B2	8/2013	Cheng et al.	
8,554,231	B2	10/2013	Jones	

**OTHER PUBLICATIONS**

International Preliminary Examination Report for PCT/IB02/00721 dated Apr. 3, 2003.

International Search Report for PCT/IB02/00721, dated Feb. 26, 2003.

Non-Final Office Action on U.S. Appl. No. 13/097,709, dated Sep. 1, 2011.

Non-Final Office Action on U.S. Appl. No. 14/058,473, dated Dec. 2, 2013.

Non-Final Office Action on U.S. Appl. No. 14/549,714, dated Nov. 18, 2015.

Notice of Allowance on U.S. Appl. No. 14/549,714 dated May 11, 2016.

Notice of Allowance on U.S. Appl. No. 12/720,862, dated Dec. 27, 2010.

Notice of Allowance on U.S. Appl. No. 13/097,709, dated Feb. 22, 2012.

Notice of Allowance on U.S. Appl. No. 13/484,583, dated Sep. 12, 2012.

Notice of Allowance on U.S. Appl. No. 13/682,230, dated Jul. 17, 2013.

Notice of Allowance on U.S. Appl. No. 14/058,473 dated Sep. 2, 2014.

Office Action on U.S. Appl. No. 12/720,862, dated Jul. 8, 2010.

Technical Report TR 23.821 V1.0.1, published Jul. 2000 by the 3rd Generation partnership Project 3GPP.

\* cited by examiner

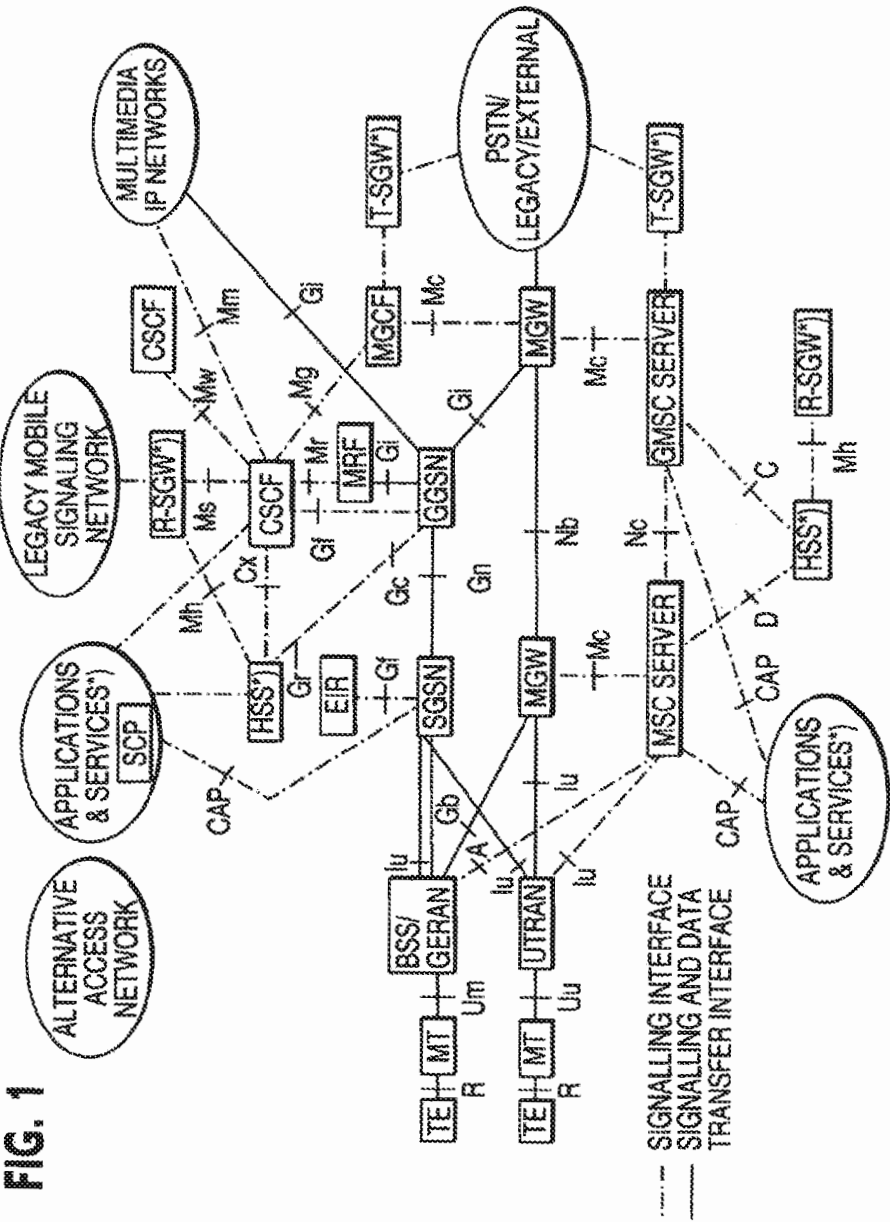


FIG. 2

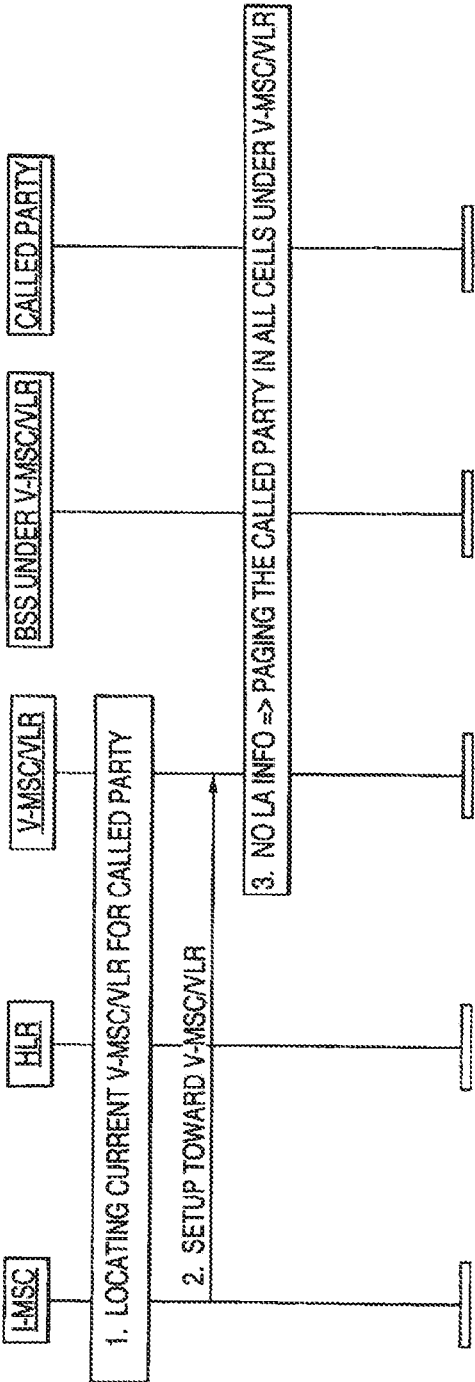
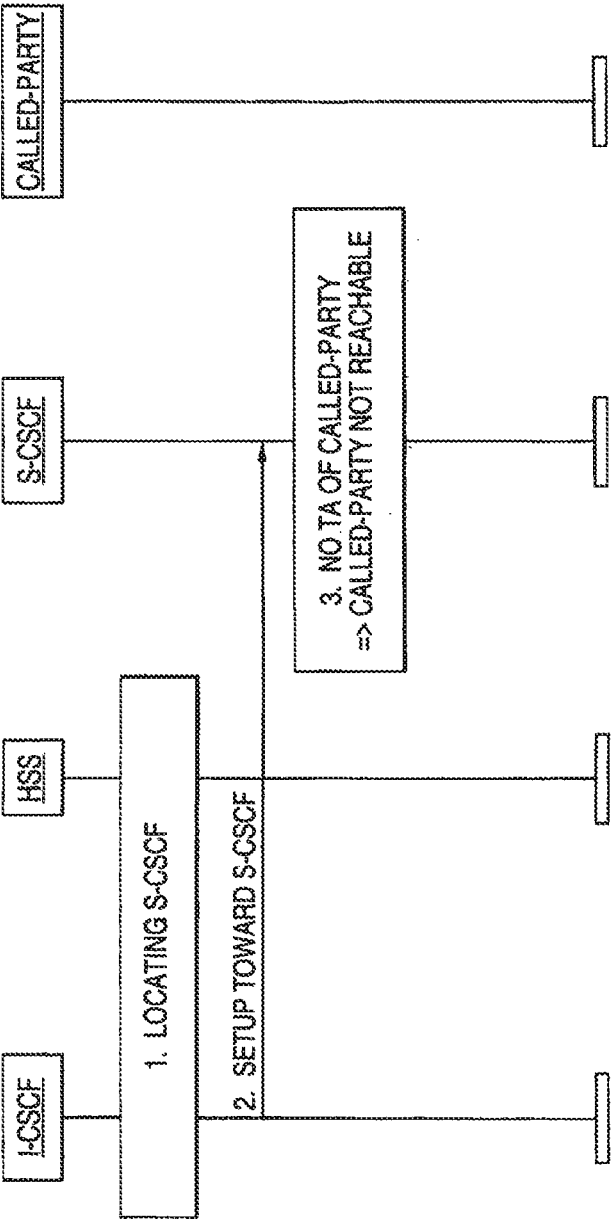


FIG. 3



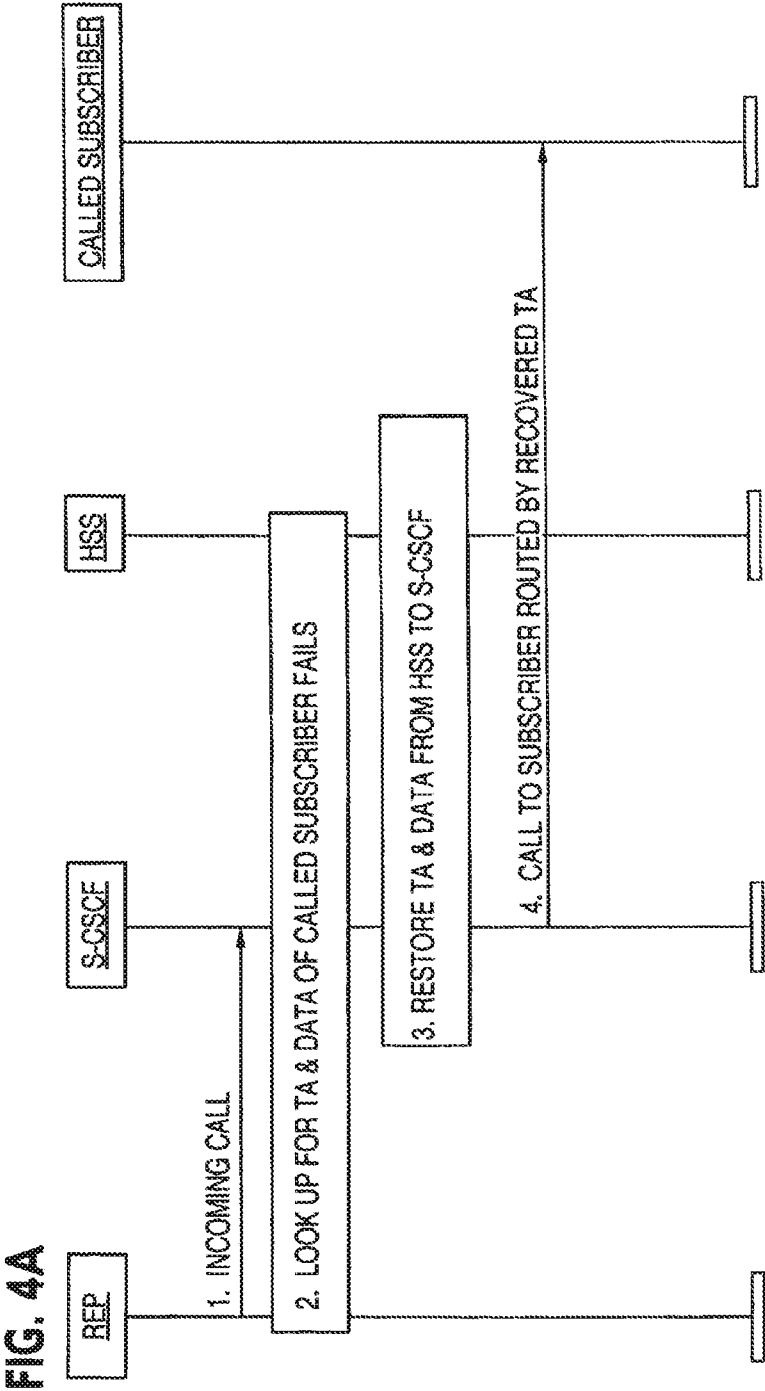
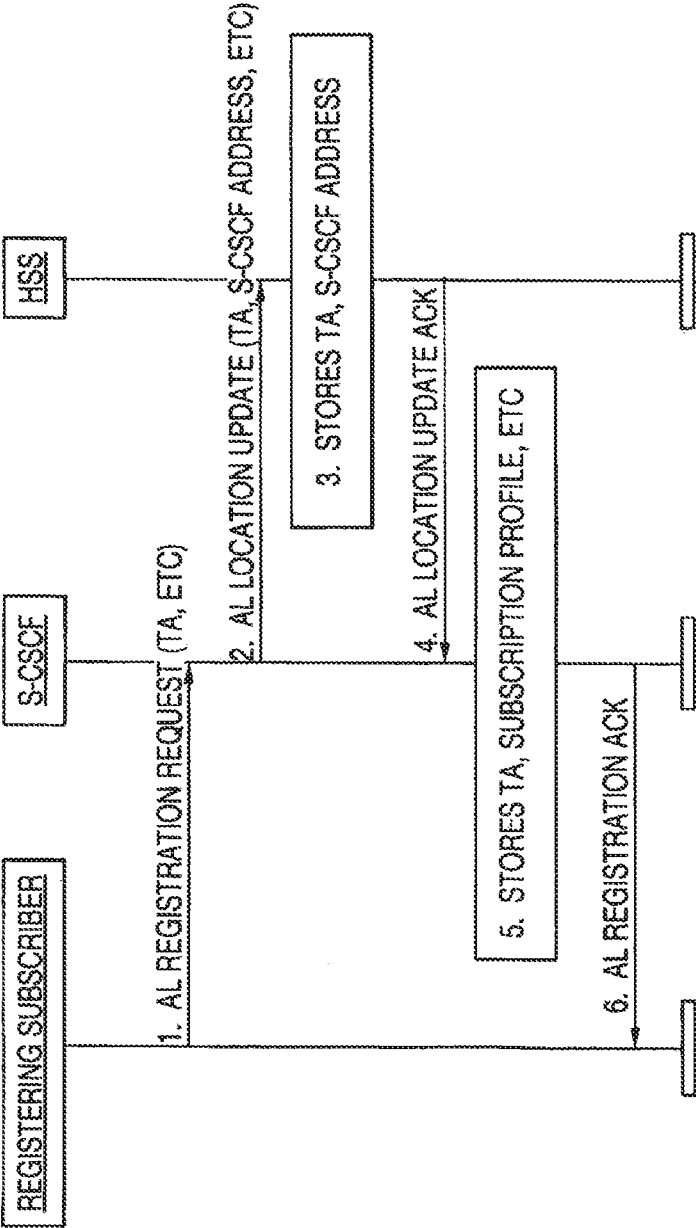
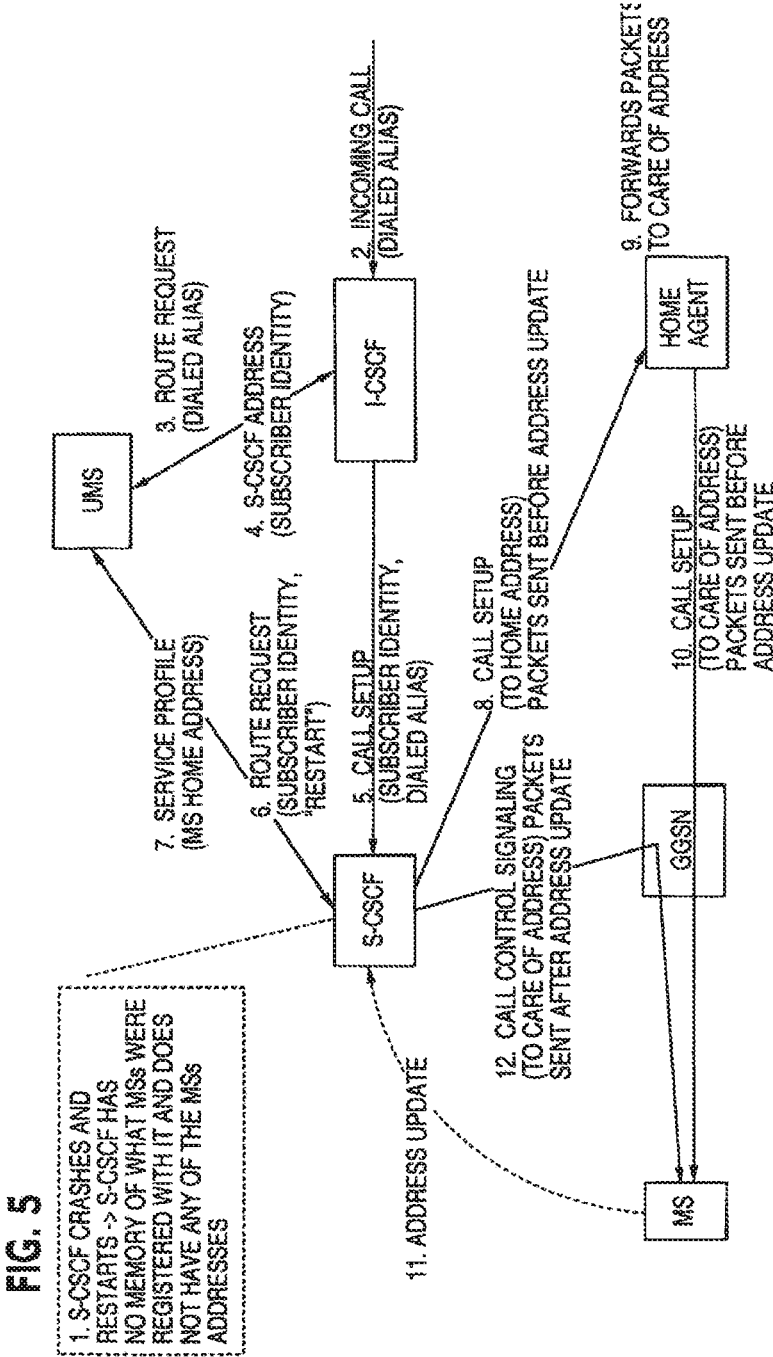


FIG. 4B







US 9,918,222 B2

1

**RECOVERY TECHNIQUES IN MOBILE NETWORKS**

**CROSS-REFERENCE TO RELATED PATENT APPLICATIONS**

This application is a Continuation of U.S. application Ser. No. 14/549,714, which is a Continuation of U.S. application Ser. No. 14/058,473, filed Oct. 21, 2013, which is a Continuation of U.S. application Ser. No. 13/682,230, filed Nov. 20, 2012 (now U.S. Pat. No. 8,600,372), which is a Continuation of U.S. application Ser. No. 13/484,583, filed May 31, 2012 (now U.S. Pat. No. 8,351,924), which is a Continuation of U.S. application Ser. No. 13/097,709, filed Apr. 29, 2011 (now U.S. Pat. No. 8,200,211, which is a Continuation-in-Part of U.S. application Ser. No. 12/720,862, filed Mar. 10, 2010 (now U.S. Pat. No. 7,937,081, which is a Divisional of U.S. application Ser. No. 09/802,861, filed Mar. 12, 2001, (now U.S. Pat. No. 7,769,374) all of which are incorporated herein by reference in their entirety.

**FIELD**

The present disclosure relates to recovery techniques for use in mobile networks. More particularly, the present disclosure relates to protecting the Transport Address (TA) which is a current Care of Address of a mobile subscriber is reachable from loss and after Call State Control Function (CSCF) crashes and after reset situations of a network element realizing CSCF functionality.

**DESCRIPTION OF RELATED ART**

Technical Report TR 23.821 V1.0.1, published July 2000 by the 3rd Generation Partnership Project (3GPP) and available on the Internet at <http://www.3gpp.org>, discloses the specifications of a 3G All-IP mobile network and this report is incorporated by reference herein in its entirety.

FIG. 1 illustrates the architecture of the network disclosed in the above-noted Technical Report. The elements shown with asterisks are elements which have been duplicated for figure layout purposes only. These duplicated elements belong to the same logical element in the reference model.

Unfortunately, the network disclosed in the Technical Report fails to include any protection of the TA of a 3G All-IP subscriber from loss. Furthermore, the network disclosed in the Technical Report fails to protect the IP address of a subscriber in the case of a reset situation of a network element realizing CSCF functionality, that is, a CSCF, thereby preventing recovery after a reset of the network element. Still furthermore, the network disclosed in the Technical Report fails to protect the location information of a subscriber after a CSCF crash, thereby preventing recovery after a CSCF crash.

**SUMMARY**

An object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL (Application Level) location update from the S-CSCF to a Home Subscriber Server (HSS) including the subscriber's TA and the (S-CSCF) address and storing data including the subscriber's TA and the S-CSCF address in the HSS so as to be protected against loss.

2

Another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including forwarding a registration request from the subscriber to an S-CSCF including the subscriber's TA and then forwarding an AL location update from the S-CSCF to an HSS including the S-CSCF address and storing data including the subscriber's TA in a non-volatile memory of the S-CSCF so as to be protected against loss.

Yet another object of the present disclosure is to provide a technique for recovering location information of a subscriber in a mobile network including upon an S-CSCF receiving a call setup request for the subscriber from an Interrogating Call State Control Function (I-CSCF), forwarding a route request to a User Mobility Server (UMS) and receiving a home address of the subscriber and then forwarding the call setup request from the S-CSCF to a home agent at the home address of the subscriber and then forwarding the call setup request from the home agent to the subscriber and subsequently forwarding an address update from the subscriber to the S-CSCF.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing and a better understanding of the present disclosure will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this disclosure. While the foregoing and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, issued a clearly understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 illustrates the architecture of a 3G All-IP mobile network.

FIG. 2 illustrates reaching a called party after losing LA (Location Area) information in a legacy mobile network.

FIG. 3 illustrates failure to reach a called party after losing TA information in a 3GPP All-IP mobile network.

FIG. 4A illustrates sending subscriber TA to S-CSCF and then forwarding it to HSS at registration.

FIG. 4B illustrates an example of reaching a called party after losing TA information in a mobile network in accordance with the present disclosure.

FIG. 5 illustrates the signal flow in the case of a recovery after a CSCF crash in accordance with another embodiment of the present disclosure.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Before beginning a detailed description of the subject disclosure, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, other components may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

In the application level of a 3G All-IP network, the reachability of a subscriber is maintained in two levels,

US 9,918,222 B2

3

namely, the network element level and the subscriber level. The S-CSCF that the subscriber is currently registered to and the TA of the roaming subscriber, which the subscriber provides to the network during Application Level (AL) registration, must be known to and maintained by the network.

Without specific support for mobility in IPv6, packets destined to a mobile subscriber would not be able to reach it while the subscriber is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a subscriber could change its IP address each time it moves to a new link, but it would then not be able to maintain transport and higher-layer connections when it changes location.

Mobile IPv6 allows a subscriber to move from one link to another without changing its IP address. A subscriber is always addressable by its "home address", an IP address assigned to it within its home subnet prefix on its home link. Packets may be routed to the subscriber using this address regardless of its current point of attachment to the Internet, and it may continue to communicate with others after moving to a new link. The movement of a subscriber away from its home link is thus transparent to transport and higher-layer protocols and applications.

A mobile subscriber is always addressable by its home address, whether it is currently attached to its home link or is away from home. While it is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if it were never mobile. Since the subnet prefix of its home address is the subnet prefix (or one of the subnet prefixes) on the subscribers' home link (it is the mobile subscribers' home subnet prefix), packets addressed to it will be routed to its home link.

While a subscriber is attached to some foreign link away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while the subscriber is visiting a particular foreign link. The subnet prefix of a subscriber's care-of address is the subnet prefix (or one of the subnet prefixes) on the foreign link being visited by it; if it is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the subscriber in its location away from home.

The association between a subscriber's home address and care-of address is known as a "binding" for the subscriber. It typically acquires its care-of address through stateless or stateful Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery. Other methods of acquiring a care-of address are also possible, such as static preassignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this discussion.

While away from home, a mobile subscriber registers one of its care-of addresses with a router on its home link, requesting this router to function as the "home agent" for it. This binding registration is done by the subscriber sending to the home agent a packet containing a "Binding Update" destination option; the home agent then replies to the subscriber by returning a packet containing a "Binding Acknowledgment" destination option. The care-of address in this binding registered with its home agent is known as the subscriber's "primary care-of address". The subscribers' home agent thereafter uses proxy Neighbor Discovery to

4

intercept any IPv6 packets addressed to the subscribers' home address (or home addresses) on the home link and tunnels each intercepted packet to the subscribers' primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation, with the outer IPv6 header addressed to the subscribers' primary care-of address.

Keeping the address of the S-CSCF ensures that a call to a subscriber can be routed to the destination node, that is, the S-CSCF. Keeping the current TA of the subscriber ensures that a call made to the subscriber which arrives at the S-CSCF can finally reach the subscriber.

As illustrated in FIG. 2, in legacy mobile networks, such as GSM, the information on the serving MSC/VLR (stored in the HLR) is adequate. That is, the called party can be reached even after the loss of the subscriber location area (LA) information by a searching/paging mechanism. In step 1, the current V-MSC/VLR for a called party is first located and in step 2 a setup toward the V-MSC/VLR is performed. In step 3, upon a loss of the LA information, the called party is paged in all cells under the V-MSC/VLR.

On the other hand, as illustrated in FIG. 3, in the 3G All-IP network, no such searching mechanism is available, so that the information of the current S-CSCF (stored in the HSS) is insufficient to reach the subscriber upon the loss of the subscriber TA. In step 1, S-CSCF is located and in step 2 a setup toward the S-CSCF is performed. However, in step 3, in the absence of the TA of the called party, the called party is not reachable.

The applicants have determined that the TA of a 3G All-IP subscriber should be protected against loss with the same level of security as that for the Serving CSCF (S-CSCF). The applicants have proposed options to protect the TA of a subscriber, namely, one option in which the TA is forwarded to the HSS and another option in which there is a security backup of the TA within the CSCF. The TA of the subscriber should be forwarded to the HSS at registration and downloaded from the HSS to the S-CSCF during recovery. Still another option is to have a permanent IPv6 (Internet Protocol Version 6) address allocated to the subscriber and to have the subscriber update its current Care-of Address (part of the TA) to the Home Agent upon obtaining the current TA.

As noted above, in accordance with the present disclosure, various options are available for implementing protection and recovery of the subscriber TA.

In the first option, as illustrated in FIG. 4A, "a safe copy" of the subscriber's TA is forwarded to the HSS for storage and protection. The TA must enjoy the same level of protection against loss as the S-CSCF address. The TA and other data can then be restored to the S-CSCF upon the earlier loss of the data by the S-CSCF. It is noted that the subscriber's TA is stored in the S-CSCF for normal operation. An incoming call from an REP (Remote End-Point) is received by the S-CSCF in step 1. In step 2, the S-CSCF looks for the subscriber's TA so as to route the call but fails to find the subscriber's TA. In step 3, the S-CSCF initiates the restoration of the subscriber's TA (and possibly other data) from the HSS. This option is only available when the S-CSCF loses only the TA of the subscriber. Finally, in step 4, the call is then routed to the subscriber using the recovered TA.

As illustrated in FIG. 4B in step 1, the registering subscriber forwards an AL registration request to the S-CSCF including the TA. In step 2, an AL Location Update is forwarded to the HSS including the TA and S-CSCF address. In step 3, the HSS stores the updated TA and S-CSCF address (in a hard disk, for example, or other non-volatile

US 9,918,222 B2

5

memory). In step 4, the HSS forwards an AL Location Update acknowledgement to the S-CSCF which stores the TA and subscription profile and other data in step 5. In step 6, the S-CSCF forwards an AL registration acknowledge to the registering subscriber.

In the second option, the same level of protection against loss applies for the subscriber's TA stored in the S-CSCF as that of the S-CSCF address stored in the HSS. For example, the subscriber's TA can be backed up in a hard disk, or other non-volatile memory in the S-CSCF.

In the case of an S-CSCF crash, when the S-CSCF restarts, all of the information regarding the mobile subscribers registered with it, including the information on how to reach the mobile subscribers, is lost. In such a situation, it is not possible to deliver mobile terminated calls to the mobile subscribers that were registered with the S-CSCF that was restarted.

In providing a solution to the above-noted problem in accordance with the third option, the following assumptions are made:

1) IPv6 is adopted for IP addressing and a subscriber is given a home address at subscription time. This home address is stored in a UMS.

2) The subscriber is in an area assigned to an S-CSCF and has registered with it and has provided its' TA, that is, the current address where the subscriber is reachable. Such an address is not the static home address but rather is the Care-of Address. Whenever the S-CSCF has to forward signaling to the mobile subscriber, it uses the Care-of Address. The subscriber has also registered its current Care of Address with its Home Agent.

3) The S-CSCF restarts due to a fault and loses the information about the mobile station.

The following procedure in accordance with the present disclosure, as illustrated in FIG. 5, may, for example, be used for mobile terminating call delivery when, as illustrated in 1, the S-CSCF crashes and restarts, the S-CSCF has no memory of what mobile stations (MSs) were registered with the S-CSCF and does not have any of the MSs Care of Address addresses:

When an incoming call at 2 reaches a CSCF in the home network, either from another IP based terminal or from an MGCF (Media Gateway Control Function), the I-CSCF queries at 3 the UMS based on the alias dialed by the calling party.

During registration, the UMS has stored information about the S-CSCF and information as to how the mobile subscriber can be reached. More particularly, the UMS has stored the address of the S-CSCF, that is, the address where CC (Call Control) signaling must be forwarded. At this point, two scenarios are possible:

The information in the UMS regarding the S-CSCF is still valid; the UMS returns at 4 the address of the S-CSCF and the Subscriber Identity and then forwards the call setup 5 to the S-CSCF.

The S-CSCF, not having information available for the alias to which the call corresponds due to a crash, queries 6 the UMS based on the Subscriber Identity optionally indicating that a restart took place in order to trigger a profile download.

The UMS returns at 7 the Home Address of the MS to the S-CSCF.

The S-CSCF forwards at 8 the signaling to the Home Address which is the home agent.

The home agent receives the packets at 9 and forwards them at 10 to the MS using the Care of Address obtained

6

during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the MS receives the first packet, it sends at 11 a message to the S-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP) and call control signalling is sent at 12 from the S-CSCF to the MS.

When the call is terminated the subscriber can optionally re-register with the S-CSCF.

2) The information in the UMS is not valid; the UMS returns the Home Address of the mobile subscriber.

The I-CSCF forwards the signaling to the Home Address.

The Home Agent receives the packets and forwards them to the Care-of Address obtained during the Mobile IP signaling exchanged when the Care-of Address was created (the usual procedure in Mobile IP).

When the mobile subscriber receives the first packet, it sends a message to the I-CSCF which sent the packet to update the address indicating the Care of Address as the correct address to be used to reach the subscriber (the usual procedure in Mobile IP).

When the call is terminated the subscriber can optionally re-register with a S-CSCF.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, drawings, and appended claims without departing from the spirit of the invention. For example, the example embodiments of the present invention have been described with respect to currently used networks, such as 313 All-IP mobile networks, and standards for simplicity. It is, of course, understood that the present invention is not limited thereto. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

1. A method comprising:

receiving a call setup request including a subscriber identity and a dialed alias for a subscriber at a serving-call state control function (S-CSCF) for call registration after the S-CSCF crashes and restarts;

sending a route request from the S-CSCF to a user mobility server (UMS) to trigger a profile download including the home address of the subscriber;

receiving the home address of the subscriber at the S-CSCF from the UMS to facilitate communication from the S-CSCF to the home address; and

sending the call setup request from the S-CSCF to a home agent at the home address of the subscriber to establish a call with a mobile station.

2. The method of claim 1, wherein the call setup request includes a subscriber identity associated with the subscriber.

3. The method of claim 2, wherein the sending a route request comprises querying the UMS based on the subscriber identity.

4. The method of claim 1, wherein the sending the call setup request comprises sending the call setup request to a care of address of the subscriber.

7

5. The method of claim 1, wherein receiving the home address of the subscriber and the sending the call setup request are performed only if information about the S-CSCF stored in the UMS is valid.

6. The method of claim 1, further comprising forwarding the call setup request to a care of address of the subscriber.

7. A non-transitory computer-readable medium having instructions stored thereon, the instructions comprising:  
instructions for receiving a call setup request including a subscriber identity and a dialed alias for a subscriber at a serving-call state control function (S-CSCF) for call registration after the S-CSCF crashes and restarts;  
instructions for sending a route request from the S-CSCF to a user mobility server (UMS) to trigger a profile download including the home address of the subscriber;  
instructions for receiving the home address of the subscriber at the S-CSCF from the UMS to facilitate communication from the S-CSCF to the home address; and  
instructions for sending the call setup request from the S-CSCF to a home agent at the home address of the subscriber to establish a call with a mobile station.

8. The non-transitory computer-readable medium of claim 7, wherein the call setup request includes a subscriber identity associated with the subscriber.

9. The non-transitory computer-readable medium of claim 8, wherein the instructions for sending a route request comprises instructions for querying the UMS based on the subscriber identity.

10. The non-transitory computer-readable medium of claim 7, wherein the instructions for sending the call setup request comprises instructions for sending the call setup request to a care of address of the subscriber.

11. The non-transitory computer-readable medium of claim 7, wherein instructions for receiving the home address of the subscriber and instructions for sending the call setup request are performed only if information about the S-CSCF stored in the UMS is valid.

12. The non-transitory computer-readable medium of claim 7, further comprising instructions for forwarding the call setup request to a care of address of the subscriber.

8

13. A system comprising:  
an interrogating-call state control function (I-CSCF) configured to:  
receive a call for a subscriber;  
send a first route request to a user mobility server (UMS);  
receive an address of a server-call state control function (S-CSCF) from the UMS; and  
send a call setup request including a subscriber identity and a dialed alias to the S-CSCF for call registration after the S-CSCF crashes and restarts; and  
the S-CSCF configured to:  
receive the call setup request from the I-CSCF;  
send a second route request to the UMS to trigger a profile download including the home address of the subscriber;  
receive the home address of the subscriber from the UMS to facilitate communication from the S-CSCF to the home address; and  
send the call setup request to a home agent at the home address of the subscriber to establish a call with a mobile station.

14. The system of claim 13, wherein the I-CSCF is configured to receive the address of the S-CSCF and to send the call setup request to the S-CSCF only if information about the S-CSCF stored in the UMS is valid.

15. The system of claim 13, wherein the S-CSCF is further configured to send the call setup request to a care of address of the subscriber.

16. The system of claim 13, further comprising the home agent, wherein the home agent is configured to receive the call setup request from the S-CSCF and forward the call setup request to a care of address of the subscriber.

17. The system of claim 13, wherein the call setup request includes the identity of the subscriber.

18. The system of claim 17, wherein the S-CSCF is further configured to query the UMS based on the identity of the subscriber.

\* \* \* \* \*

# Exhibit T

---





US00RE42883E

(19) **United States**  
 (12) **Reissued Patent**  
**Korycki et al.**

(10) **Patent Number:** **US RE42,883 E**  
 (45) **Date of Reissued Patent:** **Nov. 1, 2011**

(54) **ENHANCED PHONE-BASED  
COLLABORATION**

(75) Inventors: **Jacek Korycki**, Monmouth Junction, NJ  
 (US); **Robert Peszek**, Piscataway, NJ  
 (US); **Darek Smyk**, Basking Ridge, NJ  
 (US)

(73) Assignee: **TTI Inventions B LLC**, Wilmington,  
 DE (US)

(21) Appl. No.: **12/001,975**

(22) Filed: **Dec. 13, 2007**

#### Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **6,975,622**  
 Issued: **Dec. 13, 2005**  
 Appl. No.: **10/756,526**  
 Filed: **Jan. 13, 2004**

U.S. Applications:

(60) Provisional application No. 60/485,880, filed on Jul. 8,  
 2003.

(51) **Int. Cl.**  
**H04L 12/66** (2006.01)

(52) **U.S. Cl.** ..... **370/352; 370/260; 709/204**

(58) **Field of Classification Search** ..... None  
 See application file for complete search history.

(56) **References Cited**

#### U.S. PATENT DOCUMENTS

6,493,444	B2	12/2002	Williams	
6,690,654	B2	2/2004	Elliott et al.	
6,728,756	B1	4/2004	Ohkado	
2001/0056466	A1	12/2001	Thompson et al.	
2002/0078150	A1 *	6/2002	Thompson et al.	709/204
2002/0129106	A1	9/2002	Gutfreund	
2002/0136167	A1	9/2002	Steele et al.	
2002/0138624	A1 *	9/2002	Esenther	709/227
2002/0156671	A1	10/2002	Libra et al.	
2003/0041108	A1 *	2/2003	Henrick et al.	709/205
2003/0055893	A1	3/2003	Sato et al.	
2004/0049539	A1	3/2004	Reynolds et al.	
2004/0153504	A1	8/2004	Hutchinson et al.	
2004/0249884	A1	12/2004	Caspi et al.	

#### OTHER PUBLICATIONS

International Search Report for PCT Pat. App. No. PCT/US04/  
 21407, mailed Dec. 7, 2004.

\* cited by examiner

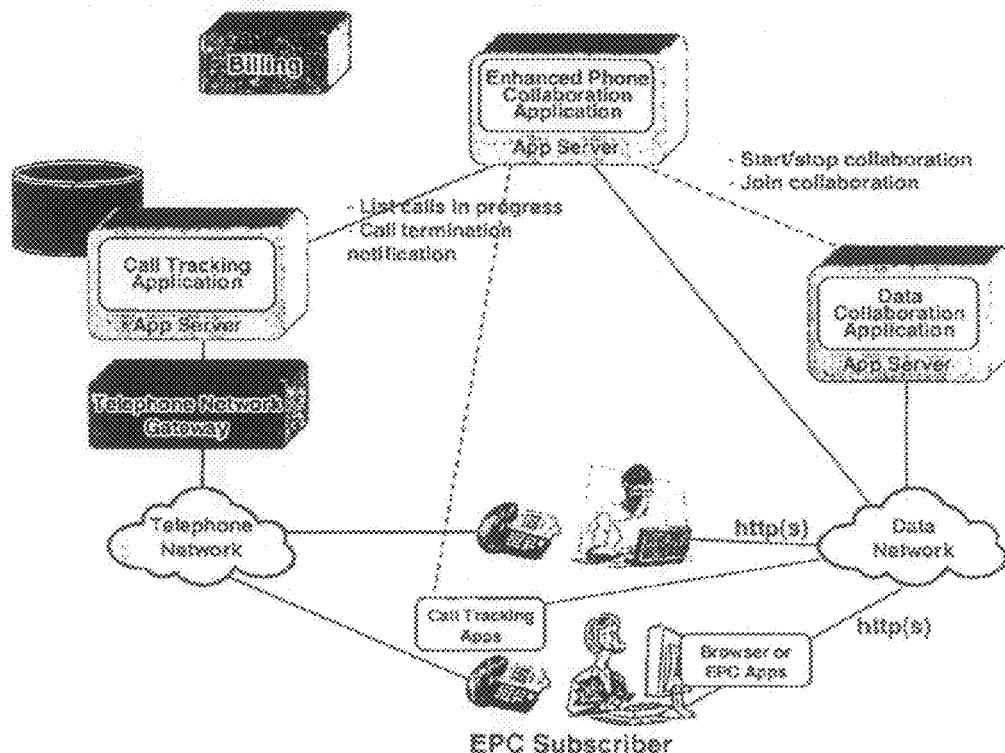
*Primary Examiner* — Phirin Sam

(74) *Attorney, Agent, or Firm* — McDonnell Boehnen  
 Hulbert & Berghoff LLP

(57) **ABSTRACT**

The present invention relates to a system and method for enhanced phone-based collaboration (EPC), which enables users to quickly and easily enhance an ongoing phone call with a variety of interpersonal real-time two-way communications (IRTC).

**9 Claims, 9 Drawing Sheets**



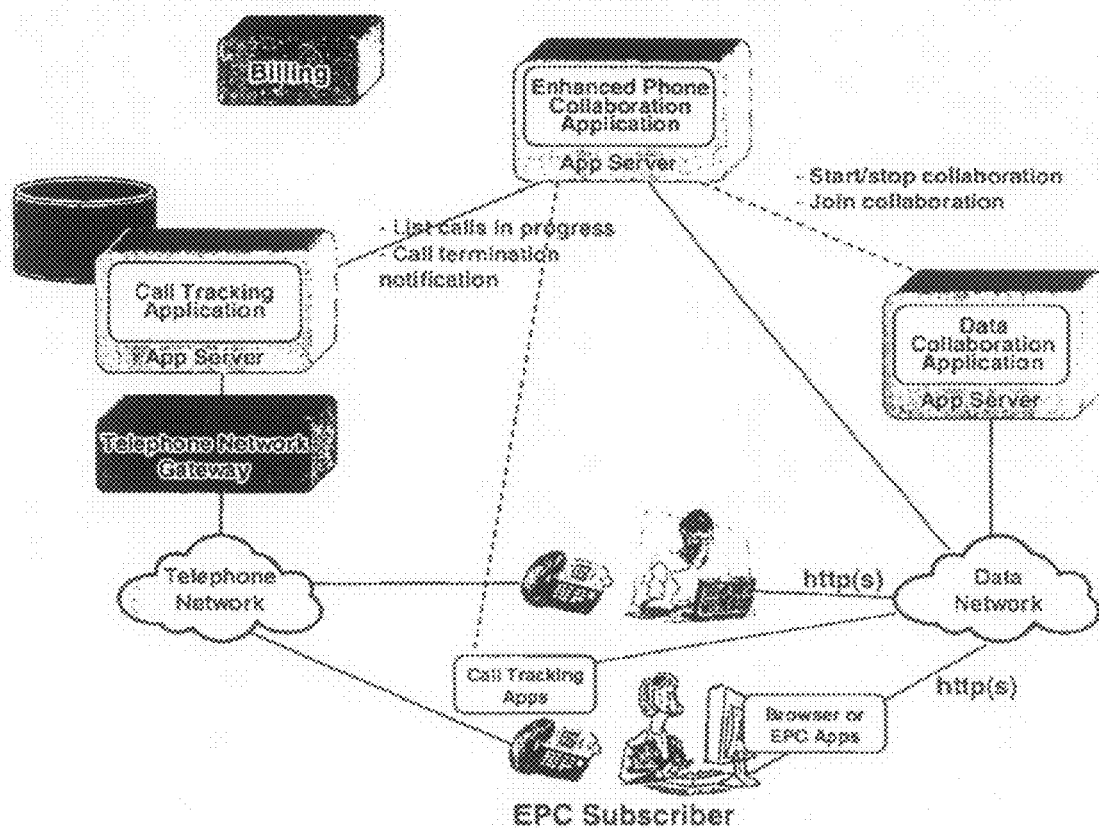


FIG. 1



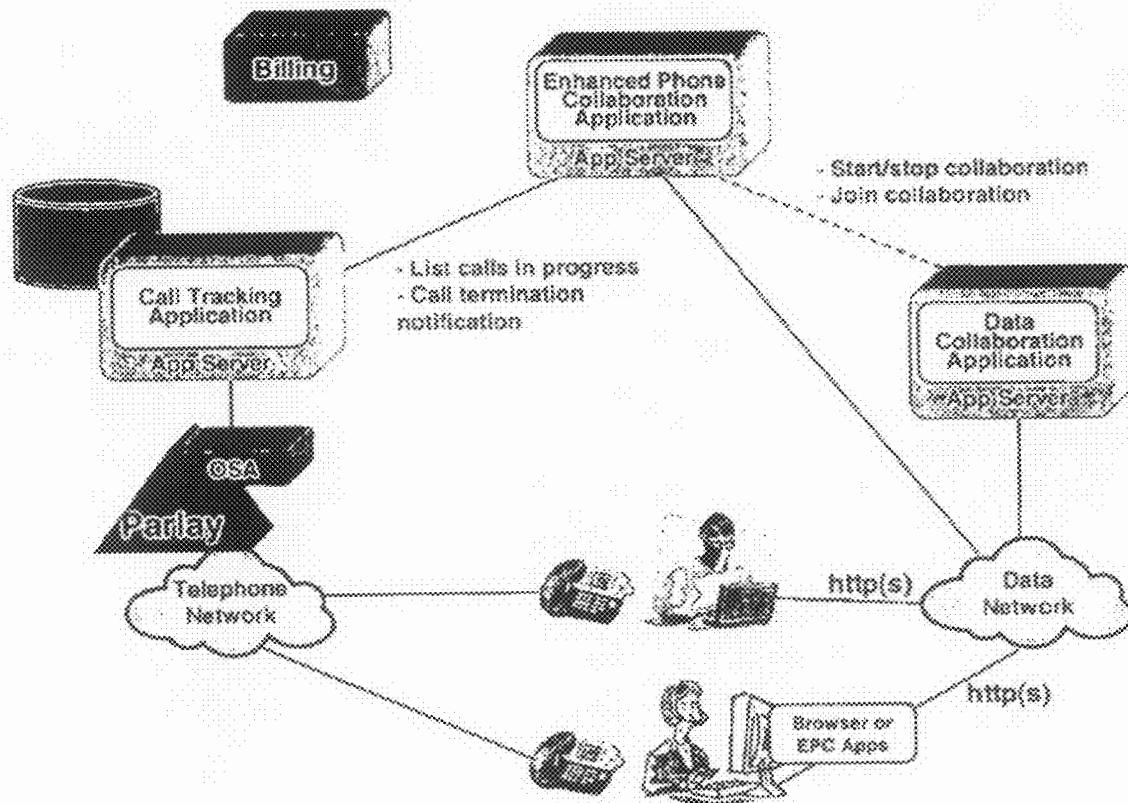


FIG. 2

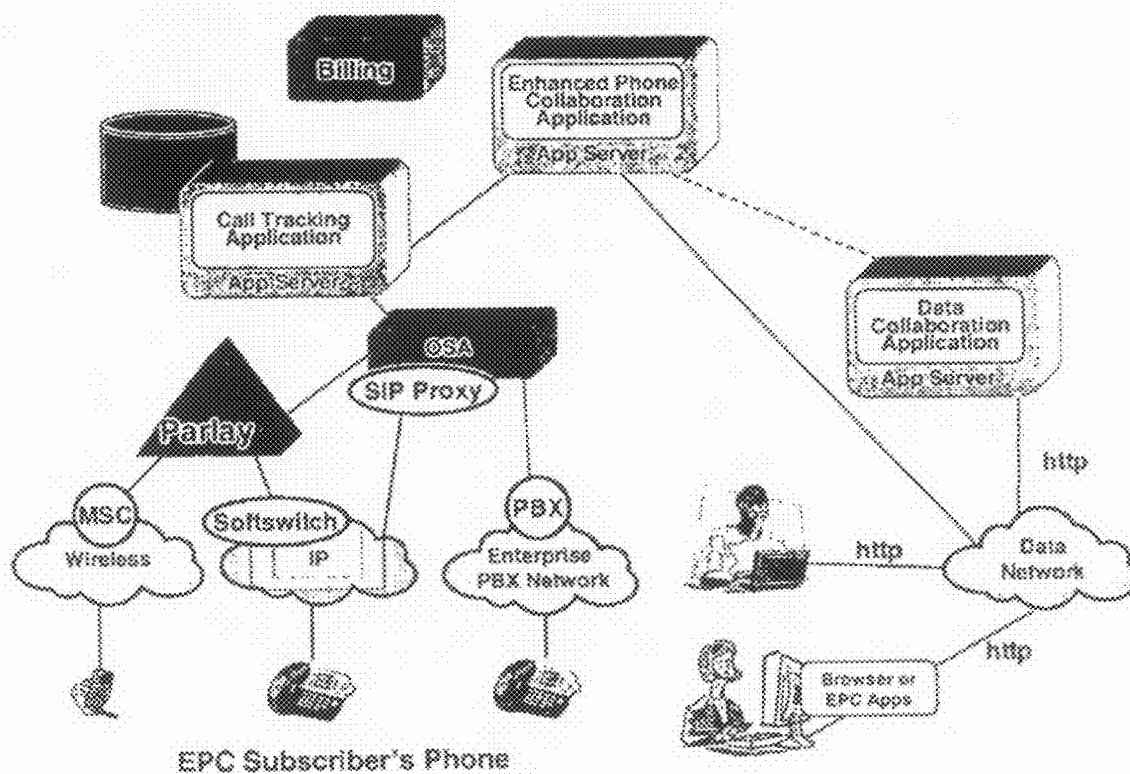


FIG. 3

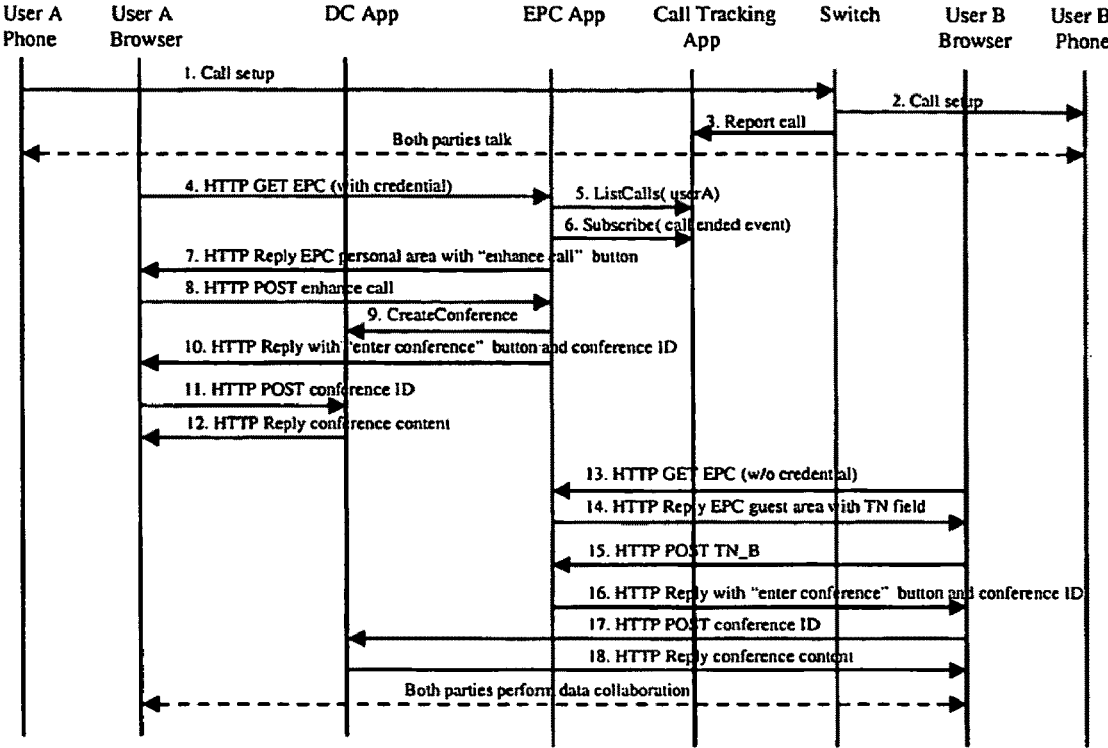


FIG. 4

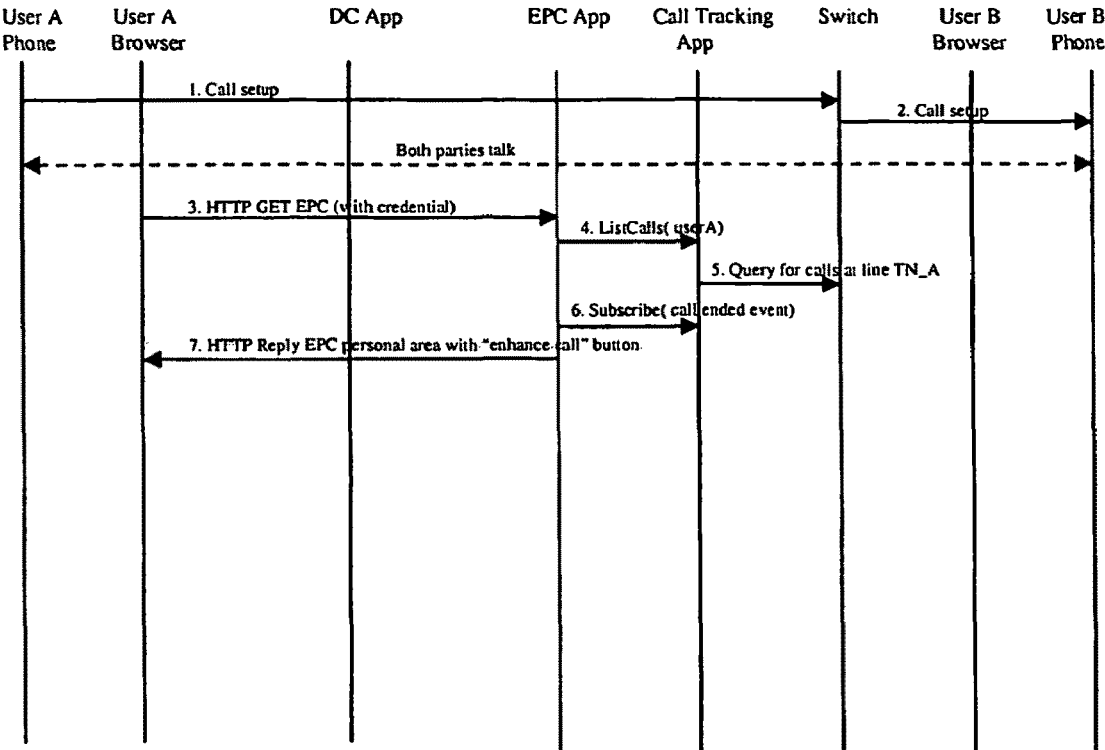


FIG. 5

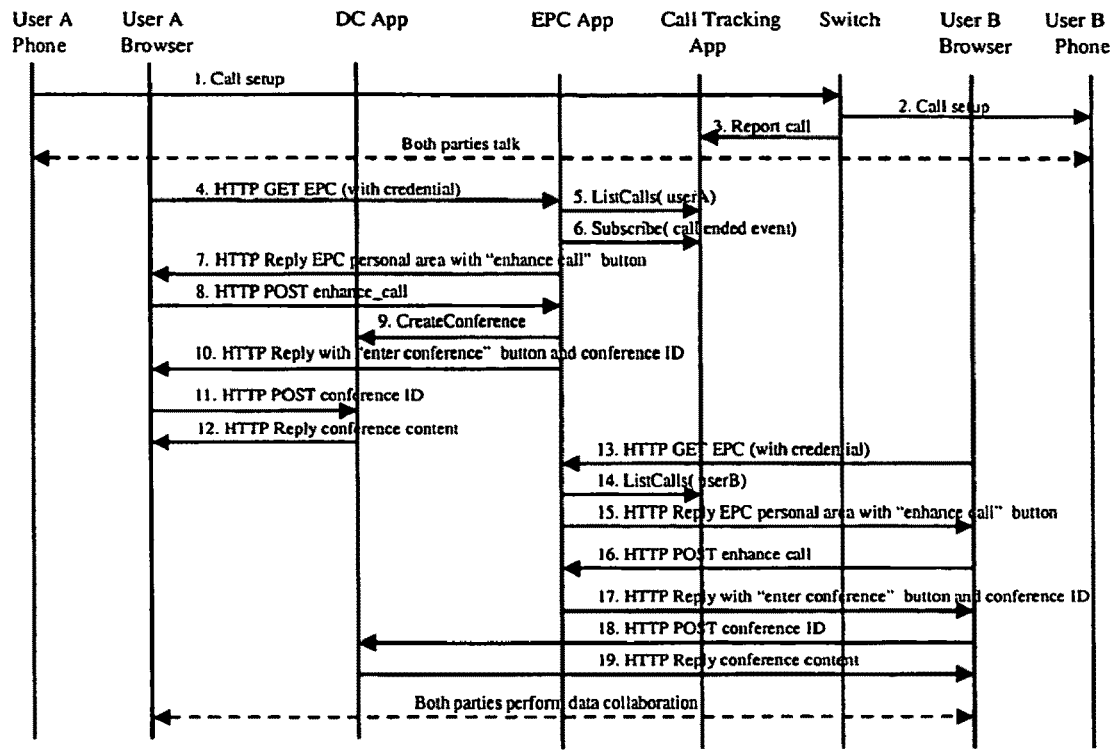


FIG. 6

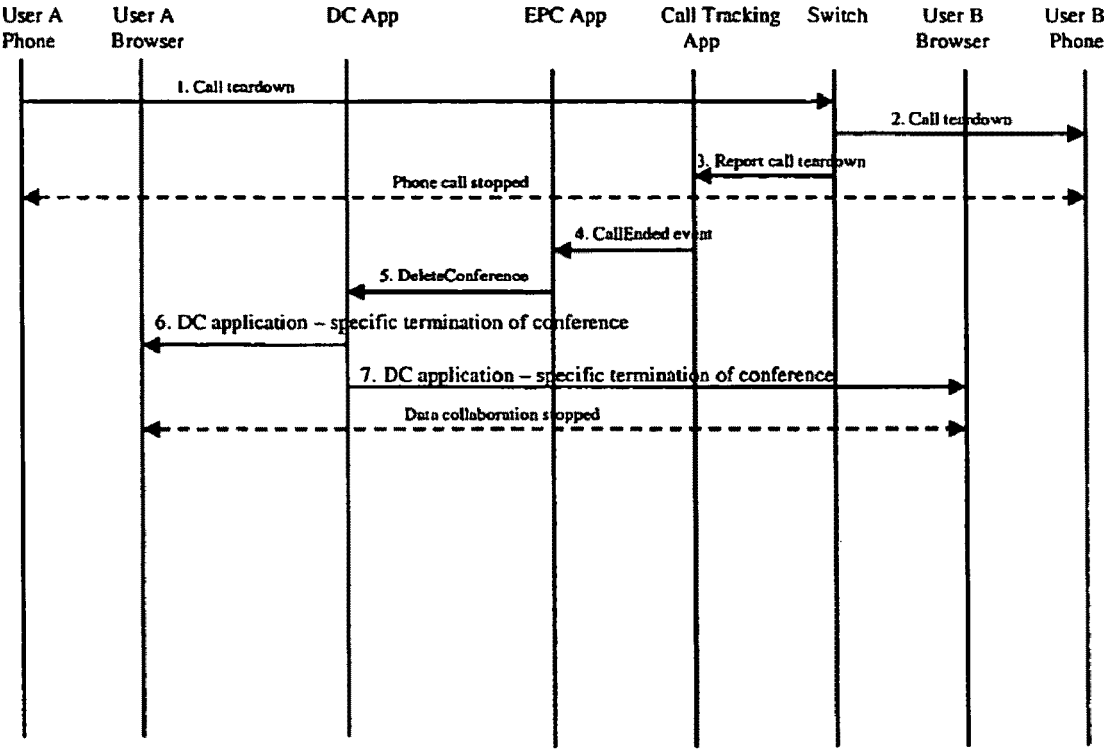


FIG. 7

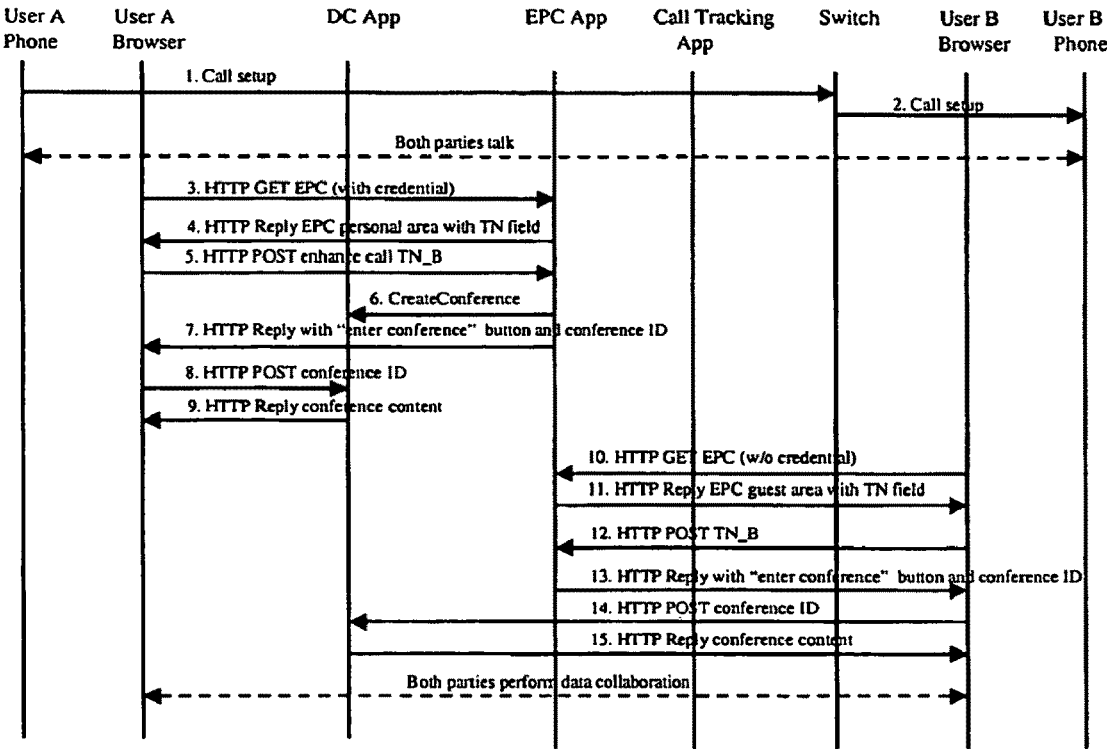


FIG. 8



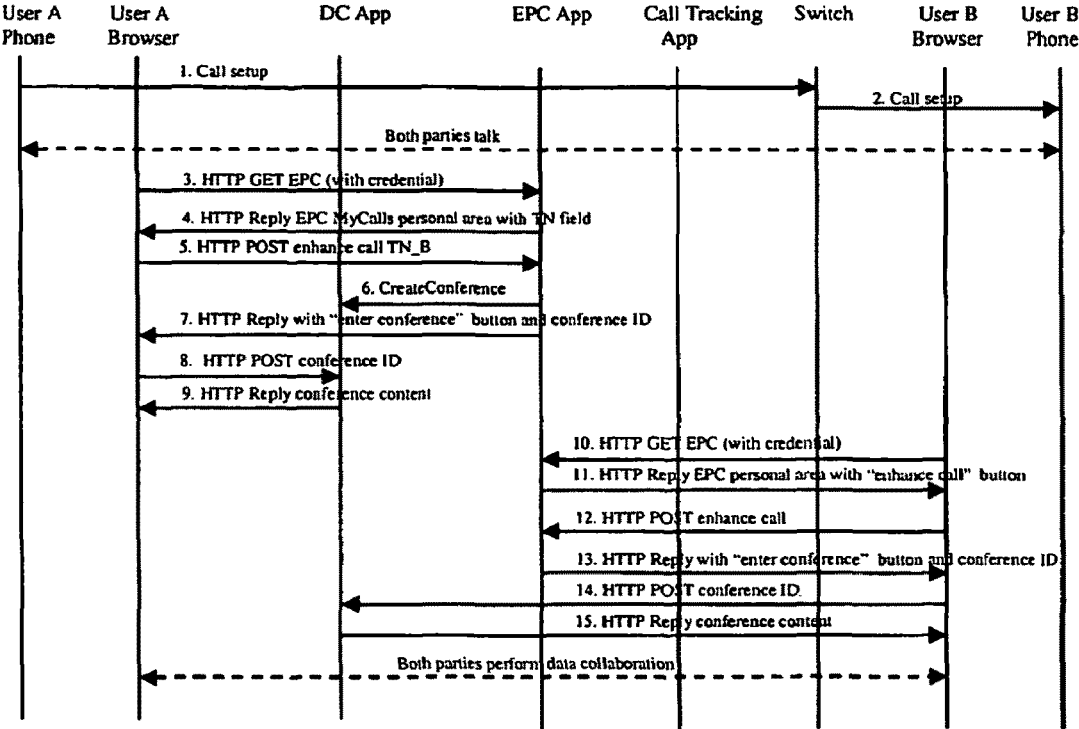


FIG. 9

US RE42,883 E

1

## ENHANCED PHONE-BASED COLLABORATION

**Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.**

### CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 60/485,880, filed Jul. 8, 2003, the contents of which are hereby incorporated by reference.

### FIELD OF THE INVENTION

The present invention relates generally to a system and method for enhanced phone-based collaboration, which allows users to more easily and securely collaborate using a variety of inter-personal real-time two-way communications media.

### BACKGROUND

Remote inter-personal real-time two-way communication (IRTC) became possible with the invention of the telephone over 100 years ago. Since then, due to technological progress, other forms of IRTC became possible. Currently, the most popular forms of IRTC include wireline and wireless telephony, audio/video conferencing, instant messaging, application sharing, desktop display sharing, whiteboard sharing, networked gaming and co-browsing. While different forms of the IRTC penetrated different markets, it is fair to say that generally telephony is pervasive in most business and personal activities while all the other forms of IRTC have a significantly smaller market penetration than telephony.

While telephony is currently the most ubiquitous and easy to use form of IRTC, end users would benefit by being able to augment a telephone conversation with other forms of IRTC. For example, during a phone conversation with a manager, a sales rep may want to jointly review and modify slides which will be presented at an upcoming client meeting. In another example, while a residential PC user talks to a software troubleshooting service representative, the user may want to add desktop sharing to the phone call in progress. In yet another example, two friends may want to jointly step through their vacation pictures while talking on the phone about recent vacations.

In all of these scenarios, communicating parties start with a simple phone call and then, as appropriate, add other forms of IRTC. As noted, currently the most common form of inter-personal real-time two-way communication is a wireline/wireless phone conversation where telephone parties use one of the following devices: a POTS phone, a PBX/CENTREX phone or a mobile phone. Other forms of IRTC, such as video conferencing, instant messaging, PC-based application sharing, desktop display sharing, whiteboard sharing, networked gaming and co-browsing, are becoming increasingly popular, but require the use of appropriate end-user devices, e.g. networked PCs, PDA's, notepads or advanced mobile phones.

One problem is that most IRTC interactions start with a regular phone call and there is no easy way to add other forms of IRTC to the phone call in progress. For example, in the scenario where a sales rep calls a manager to chat about an upcoming customer meeting and during the conversation the

2

two decide to jointly review/update presentation slides, both of the parties must have access to networked PCs in order to collaborate on the presentation. However, in a typical environment it is not easy to establish joint editing of slides. Rather, this type of collaboration is generally done completely independently from the phone call in progress. The two collaboration participants must agree on using the same collaboration application, and then establish the collaboration session, typically using a completely separate addressing schema and collaboration session establishment signaling. The complexity associated with this operation is enough to discourage all but the most technically inclined end users.

In another example, similar difficulties arise when two friends while talking on the phone about their recent vacations would like to jointly view sets of vacation pictures. In a still further example, a house seller and real estate attorney lawyer having a phone conversation about the results of a home inspection decide to jointly prepare a response to the buyer's long list of repair requests. As with the above examples, there is no easy way to add collaborative document viewing and editing.

In particular, upon user A and user B agreeing to enhance the phone call, they must also agree on which software product will be used to enhance the phone call. This decision may require a technical savvy of network, firewall/NAT infrastructure that affects many of the existing software products. Some of the known choices include T.120 clients such as NetMeeting, IM products such as Yahoo! Windows Messenger, etc., and existing web conferencing solutions such as DCL Meeting Server, WebEx, etc.

To utilize these software products, users must have access to the software, which may require purchasing the software, software installation and establishing a billing agreement between the users and the service provider. Then the collaboration session must be established. This is accomplished by setting up the enhanced session manually using tools provided by the corresponding product, exchanging the information required to connect to the session and manually entering the information in the corresponding application. Such information may include IP addresses (NetMeeting or other T.120 clients), subscription IDs (IM products), and Conference Server URL with tokens such as conference key, and password (web conferencing solutions).

Exchanging the information necessary for entering the collaboration may further entail the web conference providers sending the information by e-mail distribution. While this procedure is viable for conferences scheduled in advance, this approach lacks real time characteristics required for ad-hoc spontaneous call enhancement.

Many of the current methods of enhancing the phone call are cumbersome and are not practical unless both users already subscribe to the same service and have already installed the corresponding software. Even if software installation and service subscription are not issues, the collaboration setup process involves many manual steps that diminish both usefulness and accessibility.

The manual process requires, at minimum, the users to perform session signaling twice: first using phones and phone numbers, then using PC based collaboration application and it's proprietary session signaling and addressing. However simple the application signaling is, it requires effort and needs to be learned by the users.

Therefore, there remains a need in the art for improvements in the technology of enhanced phone-based collaboration.

### SUMMARY

The present invention describes the solution to enable the above types of scenarios, as well as others. The present inven-

US RE42,883 E

3

tion provides end users with an easy and convenient way to augment phone conversations with other forms of communication and collaboration. Further, the present invention provides telephone service providers with an opportunity to expand their offering of value added services.

The present invention provides a system and method for Enhanced Phone-based Collaboration (EPC) service that will enable telephone parties to easily and conveniently add other IRTC applications for collaboration by leveraging the phone call already in progress. In particular, in accordance with the present invention, to start the collaboration, the telephone parties would only need to identify the phone call in progress, which they want to enhance. The present invention will be more fully described below with reference to the Drawing Figures.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 depicts high-level implementation architecture for EPC in accordance with one embodiment of the present invention.

FIG. 2 depicts sample implementation architecture for EPC in accordance with an embodiment of the present invention utilizing wireline PSTN.

FIG. 3 depicts sample implementation architecture for EPC in accordance with an embodiment of the present invention utilizing wireless PSTN, PBX or IP phones.

FIG. 4 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating and have access to full telephony integration.

FIG. 5 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating and have access to full telephony integration, but without intelligent network (IN) triggers.

FIG. 6 shows a call flow for a scenario according to the present invention wherein two subscribers are collaborating and have access to full telephony integration.

FIG. 7 shows a call flow for a scenario according to the present invention that provides for automated stopping of the data collaboration conference.

FIG. 8 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating but do not have access to full telephony integration.

FIG. 9 shows a call flow for a scenario according to the present invention wherein two subscribers are collaborating but do not have access to full telephony integration. FIG. 1

#### DETAILED DESCRIPTION OF THE DRAWINGS

The EPC service according to the present invention enables users, which participate in a phone call; to enrich their communication with a variety of PC based applications. The EPC service of the present invention bridges existing technologies to provide a simple and straightforward experience to the users, which overcomes the disadvantages, noted above with respect to known methods and services.

The method and system of the present invention provides a much simpler and more spontaneous means for establishing collaboration. In particular, a subscriber needs only to establish a phone call and the enhancement can be achieved by using a choice driven web page. The users do not need to learn the application specific signaling, nor do they need to enter any application specific remote address. Even if there is only one subscriber on the call, the process is simplified. The

4

non-subscriber simply needs to enter his own phone number. There is no need for the non-subscriber to learn application specific signaling.

In addition, the EPC service of the present invention provides a benefit to service providers, application developers, and end customers. For example, the EPC service of the present invention defines an open architecture allowing third party integration of an arbitrary form of IRTC (such as a third party network game) with a phone call. This gives motivation for application development of new forms of IRTC and may open new revenue streams for the service provider. The EPC services of the present invention allow service providers to offer a variety of user-friendly phone call enhancements accessible to a broad customer base by utilization of both a large customer base and common billing structure. Application developers are attracted by a large customer base willing to use their services and common billing infrastructure, which simplifies the complexity of applications and reduces development cost. Customers can enjoy a user-friendly interface, a variety of new forms of IRTC, and convenience of maintaining only one account with one password to remember and a single bill from a single Service Provider.

The present invention will be described in detail with reference to the drawing figures. Initially, it is noted that while the description and drawings show implementation scenarios for PC-based collaboration, that the present invention applies equally to other interactive networked devices, such as PDAs, notepads, advanced mobile phones, etc. Further, for simplicity, the description and drawings show implementation in the context of a two party call, but the present invention applies equally to enhancement of multi-party or conference calls.

The present invention provides a system and method for EPC service that will enable telephone parties to easily and conveniently add other IRTC applications for collaboration by leveraging the phone call which is already in progress. In particular, in accordance with the present invention, to start the collaboration, the telephone parties would only need to identify the phone call in progress, which they want to enhance. However, the user experience will vary depending on whether the user subscribes to an EPC service. Therefore, the present invention is described below for both scenarios in which there is only one subscriber and in which both parties are subscribers. Further, several different implementation schemes will be described for both scenarios.

In a first scenario, both parties subscribe to the EPC service and implementation of the EPC service can be carried out via a browser with full telephony integration; via a browser with limited telephony integration; via an application with full telephony integration; or via an application with limited telephony integration.

For example, in a browser-based implementation with full telephony integration, either subscriber may use their favorite browser to access an EPC service site. After successfully authenticating the initiating subscriber, the browser displays the list of that subscriber's phone calls in progress. The initiating subscriber clicks on a particular call on the list in order to add enhanced collaboration to that call. Optionally, the collaboration automatically terminates when the associated phone call is terminated.

In a further example, using a browser-based implementation with limited telephony integration, either subscriber may use their favorite browser to access an EPC service site. After being successfully authenticated by the service provider, the initiating subscriber enters the other parties' telephone number and clicks on a "start to collaborate" button. It is important to note that for this scenario and implementation, either subscriber can initiate the collaboration.

## US RE42,883 E

5

Moreover, in an application-based implementation with full telephony integration, either subscriber may start the EPC application. After successfully authenticating the initiating subscriber, the application displays the list of that subscriber's phone calls in progress. The initiating subscriber clicks on a particular call on the list in order to add enhanced collaboration to that call. Optionally, the collaboration automatically terminates when the associated phone call is terminated. It is important to note that for this scenario and implementation, either subscriber can initiate the collaboration.

In another example, for an application-based implementation with limited telephony integration, either subscriber may start the EPC application. After being successfully authenticated by the service provider, the initiating subscriber enters the other parties' phone number and clicks on a "start to collaborate" button. It is important to note that for this scenario and implementation, either subscriber can initiate the collaboration.

In a second scenario, only one party subscribe to the EPC service, however, implementation of the EPC service can be carried out in any one of the implementations noted above; i.e. via a browser with full telephony integration; via a browser with limited telephony integration; via an application with full telephony integration; or via an application with limited telephony integration.

For example, in a browser-based implementation with full telephony integration, the subscriber may use a favorite browser to access an EPC service site. After successfully authenticating the subscriber, the browser displays the list of the subscriber's phone calls in progress. The subscriber clicks on a particular call on the list in order to add enhanced collaboration to that call. Optionally, the collaboration automatically terminates when the associated phone call is terminated.

In a further example, for a browser-based implementation with limited telephony integration, the subscriber may use a favorite browser to access an EPC service site. After being successfully authenticated by the service provider, the subscriber enters the other parties' telephone number and clicks on a "start to collaborate" button.

In an additional example, for an application-based implementation with full telephony integration, the subscriber may start the EPC application. After successfully authenticating the subscriber, the application displays the list of the subscriber's phone calls in progress. The subscriber clicks on a particular call on the list in order to add enhanced collaboration to that call. Optionally, the collaboration automatically terminates when the associated phone call is terminated.

Moreover, for an application-based implementation with limited telephony integration, the subscriber may start the EPC application. After being successfully authenticated by the service provider, the subscriber enters the other parties' phone number and clicks on a "start to collaborate" button.

As noted above, if both parties are subscribers, either party may initiate the collaboration. However, a non-subscriber will be able to collaborate only upon an explicit invitation by the EPC subscriber. In particular, during the phone conversation the EPC subscriber will invite the non-subscriber to collaborate and provide instructions on how to the non-subscriber can join collaboration session using an off-the-shelf Internet browser. For example, the EPC subscriber will provide the non-subscriber with a guest page URL over the phone, or by an e-mail message, etc. (such as [www.service-provider.com/epcguest](http://www.service-provider.com/epcguest)). To start collaboration the subscriber simply enters both parties' phone numbers and clicks on a "start to collaborate" button.

6

FIG. 1 depicts high-level implementation architecture for EPC in accordance with one embodiment of the present invention. In particular, the architecture in FIG. 1 comprises the following components.

Telephone Network—This network may be circuit switch based (e.g. AIN PSTN network) or packet based (e.g. IP network with SIP or H.248 based phones). The network may be the Public Telephone Network or a private enterprise network.

Call Tracking Application—This application keeps track of the EPC subscriber's telephone calls in progress and may be network server based or CPE-based. For example, the server based Call Tracking Application could track calls in the PSTN via a Parlay-based PSTN Gateway or for wireless phone based application could track calls originating/terminating from/on the given wireless phone device. The Call Tracking Application supports an interface for external application, such as the EPC application, to retrieve calls in progress and optionally receive notifications about call termination.

Telephone Network Gateway—The gateway provides the Call Tracking Application with information necessary to perform call tracking. For example, a Parlay-based Telephone Network Gateway would provide the Call Tracking Application with notifications about establishment/termination of telephone calls.

Data Network—This is a packet-based network, e.g. IP network. Therefore, in the case of packet-based telephony the Telephone Network and Data Network can be the same IP based network.

Data Collaboration Application—This application supports real-time data collaboration, (e.g. video conferencing, instant messaging, PC-based application sharing, desktop display sharing, whiteboard sharing, networked gaming and co-browsing). This application could be server and/or CPE (e.g. PC, notepad, PDA) based. For example, the Data Collaboration Application could be server based and utilize T.120 protocols to support application sharing, in which case, the user device based portion of the Data Collaboration Application may include only an Internet browser executing a data collaboration applet, downloadable on demand.

Enhanced Phone-based Collaboration Application—This application supports a seamless transition from a simple phone call to a phone call extended with data collaboration. When the EPC subscriber invokes the EPC Application, the application first obtains the list of calls in progress from Call Tracking Application and presents the subscriber with a list of calls suitable for enhancement with data collaboration. After the EPC subscriber chooses the call for enhancement, the EPC signals to the Data Collaboration Application to establish the data collaboration session. In the case, where the Call Tracking Application is not capable of providing the full information about the calls in progress (e.g. due to the blocked caller ID), the EPC Application provides the EPC subscriber with the means to manually enter the information about the call to be enhanced. After the Data Collaboration Application establishes the data collaboration session for the EPC subscriber, it provides the other telephone party(s) with the means to join the data collaboration session.

FIG. 2 depicts sample implementation architecture for EPC in accordance with an embodiment of the present invention utilizing wireline PSTN. The architecture shown in FIG. 2 contains the same components as those shown in FIG. 1, however, in FIG. 2, the Network Gateway comprises an OSA/Parlay call control interface, such as the ISCP/OSG product of Telcordia Technologies, Inc. This call control interface



## US RE42,883 E

7

provides a server based Call Tracking Application with notifications necessary to track PSTN calls.

FIG. 3 depicts sample implementation architecture for EPC in accordance with an embodiment of the present invention utilizing wireless PSTN, PBX or IP phones. In this architecture, the Call tracking Application is also server based and tracks calls via a standardized OSA/Parlay call control interface, such as that implemented by the ISCP/OSG product of Telcordia Technologies, Inc. The call control interface supports interfaces specific to particular telephone network implementations, such as MSC, soft switches or PBX phones.

General call processing flows representing service execution scenarios for the implementation architecture depicted in FIG. 2 are described below. In particular, scenarios where only one or both communicating users subscribe to the EPC service are described as well as scenarios based on whether real-time call information is available from the telephone network.

The EPC service may be made available using either a standard web browser or a service-specific client application that subscribers would need to install before using the EPC service. The scenarios below focus on the web browser case. However, the application case is similar, with the browser interface replaced by the client application-specific interface (such as web services, sockets etc.) over which similar data content flows.

Further, for the scenarios discussed, the Data Collaboration Application is browser based, i.e., it can be easily accessed by anyone with a web browser connected to the IP network. Standard HTTP Requests can be used to access the EPC service. The choice of HTTP Requests is an implementation decision for both the EPC application and Data Collaboration Application. While HTTP POST and HTTP GET represent typical uses, the present invention is not so limited and other alternative requests can be utilized. In this example, HTTP GET is used for loading of an EPC web page and HTTP POST is used for form-based actions following a user input.

Further, all HTTP messages could be secured if HTTPS is used instead of plain HTTP, at the cost of some performance degradation. Therefore, in the following description, all references to HTTP mean that HTTPS could be alternatively used in its place.

The EPC service may be implemented with a variety of interfaces between server side components and the discussion below assumes the following server side interfaces.

The Call Tracking Application exposes a web service consumed by the EPC application and allows for listing current subscriber's calls, and registering for and receiving call tear-down notification.

The Data Collaboration Application exposes a web service consumed by the EPC application and allows creation and deletion of a data collaboration conference.

The present invention is not limited to web services for the server side component interfaces, but rather includes other distributed computing technologies, such as CORBA, DCOM, Java RMI etc.

Based on the assumptions noted above, the flows that follow describe only one possible implementation choice, i.e. that shown in FIG. 2. The technical detail provided is not essential to the EPC service but makes the description consistent.

The EPC service offers most of its advantages with full telephony integration, wherein creation and access to data conference is automated based on information already present in the telephone network. This information includes the telephone call; the associated parties that already agreed to participate in the call and the timing of the call.

8

Further, the EPC service is most valuable if both users subscribe to the service. However, the EPC service is still valuable if only one user subscribes. Since in the initial phase of the service deployment a single subscriber scenario is more likely to occur, descriptions for both single subscriber and two subscribers follow.

FIG. 4 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating and have access to full telephony integration.

Step 1. User A (the subscriber) initiates a telephone call to user B (not a subscriber). This is a simplified and abstracted signaling that may take different forms in different telephony environments (PSTN, VoIP, PBX etc), however, full details are not essential to the EPC service.

Step 2. User B answers the call. It is irrelevant which user initiates the call, e.g., the call might have been initiated by user B and answered by user A.

Step 3. The switch reports the call to the Call Tracking Application (for example utilizing Parlay interface of the ISCP node). This is one possible variant based on registering a trigger for the subscriber telephone line. A trigger-less variant is also possible and described in more detail below.

Step 4. During the telephone call, both parties agree to enhance the call with data collaboration features using standard web browsers on their PCs. User A, the subscriber loads the EPC web page into the browser. The browser could optionally authenticate user A as a subscriber or automate the step by passing pre-stored subscriber credentials in a way standard for web based personalized services.

Step 5. Recognizing user A as a subscriber, the EPC Application invokes a ListCalls web service on the Call Tracking Application querying for calls currently in progress that involve user A. The web service call returns information about the call between user A and user B. This information includes user B telephone number TN\_B. The EPC Application stores this information in preparation for establishing a data conference.

Step 6. This step is an optional step in which the EPC Application invokes a web service in order to register for call tear down notification from the Call Tracking Application (which in turn performs appropriate registration depending on the particular telephony environment, e.g., utilizing Parlay interface of the ISCP node). This step is optional and performed only if automated conference stopping is required by the service or users and implemented by the Data Collaboration Application.

Step 7. In response to the original web page request of user A, the EPC Application returns a personal EPC web page to user A that includes information about the current call and the "enhance call" button.

Step 8. User A clicks on the "enhance call" button, which generates an HTTP POST message to the EPC Application.

Step 9. In another optional step, the EPC Application creates a new instance of data collaboration conference. This is accomplished by invoking a web service exposed by the Data Collaboration Application. As a result of this step a conference ID is established either by the EPC Application or by the Data Collaboration Application. This conference ID could take many different forms depending on the particular Data Collaboration Application, e.g. it could be a pair of conference reference number and PIN number. This step is optional and may not be required if the Data Collaboration Application creates a new instance automatically when the first conference participant joins.

Step 10. The EPC Application returns a confirmation page to user A with the "enter conference" button together with

## US RE42,883 E

9

associated information (using HTML form mechanism) consisting of the Data Collaboration Application network address, conference ID established in step 9 and user A's full name to be used as conference participant identifier. Only the "enter conference" button is rendered visibly to the user, the rest of the information is hidden.

Step 11. User A clicks the "enter conference" button which generates an HTTP POST message directly to the Data Collaboration Application with enough information to allow user A's participation in the instance of data collaboration conference.

Step 12. The Data Collaboration Application returns Data Collaboration specific content including active content that loads into user A's browser realizing start of his/her participation in a data conference.

Step 13. When user A's participation in data conference is completed, user A informs user B over the telephone call that user B may enter a conference via the main EPC web page. Preferably the main EPC URL is easy to memorize and enter into a browser, e.g. epc.com. User B loads the main EPC page using a standard browser.

Step 14. Since user B is not a subscriber, no credentials are passed and a public guest area is loaded into user B's browser. This web page offers a guest user a way to enhance a phone call with the service subscriber by obtaining guest user's telephone number (telephone number edit field and the "enhance call" button). Knowledge of one's own telephone number and the time window of the telephone call are the only prerequisites for a guest user to enter a data collaboration conference with a subscriber.

Step 15. User B enters his/her own telephone number TN\_B and clicks "enhance" call button generating an HTTP POST message to the EPC Application with TN\_B information.

Step 16. The EPC Application correlates TN\_B with the call and conference it keeps track of. It returns the same confirmation web page with the "enter conference" button as it did to user A in step 10. In particular it includes conference ID identifying the data conference user A is already participating in waiting for user B to arrive.

Step 17. User B clicks the "enter conference" button generating HTTP POST message directly to the Data Collaboration Application that transmits the conference ID and user B's telephone number to be used as data conference participant identifier.

Step 18. The Data Collaboration Application returns Data Collaboration specific content including active content that loads into user B's browser realizing the start of participation in a data conference. Users A and B immediately "see" each other in that conference (user A's name and user B's telephone number are passed to the Data Collaboration Application as participant identifiers). With the conference established, while still talking on the phone, user A and user B can now engage in data collaboration as implemented by the Data Collaboration Application (e.g. white boarding, app sharing, gaming etc.)

In another embodiment of the present invention, steps 8-12 above could also be optimized and performed in a way requiring only a single button click from a user.

As indicated in the description of step 3 of the above flow, a variant flow is possible depending on details of telephony integration. In particular, instead of the Call Tracking Application requiring triggers for telephone line of each EPC subscriber, it is possible to implement a trigger less variant if the telephone network allows to query in real-time for call information.

10

FIG. 5 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating and have access to full telephony integration, but without IN triggers. Only a few of the steps of the flow are shown, so as to focus on the differences from that shown in FIG. 4.

Steps 1-2. Phone call setup between users A and B. The switch does not report the call as no trigger is maintained.

Step 3. User A, the subscriber loads the main EPC web page.

Step 4. The EPC Application obtains call information for user A by invoking ListCalls web service of the Call Tracking Application.

Step 5. The Call Tracking Application obtains information asked by the EPC Application by itself querying the telephone network supplying the user A's line number TN\_A. This could take many different forms depending on the particular telephone network and involve different telephone network elements, e.g. the ISCP node.

The rest of the steps remain the same as those described for FIG. 4.

In the event that both users are subscribers to the EPC service, the experience of both users is symmetrical and may be fully automated. Neither user needs to enter a telephone number as such information is already tracked by the EPC service. A number of implementations are possible where both users are subscribers. For example, the sequence in which the users join the data conference may be synchronized so that the calling user needs to establish a conference first before the called user can join. This could be appropriate if the calling user is billed for the data enhancement and no conference can be created without that user's initiative. However, it is also possible for both users to initiate call enhancement at the same time and the data conference could be created by whoever gets to that point faster. For simplicity, in the flow description of FIG. 6, user B joins the data conference after user A.

FIG. 6 shows a call flow for a scenario according to the present invention wherein two subscribers are collaborating and have access to full telephony integration.

Steps 1-12. The telephone call is established and user A enhances the call. These steps are identical to the one subscriber case described in FIG. 4. The telephony integration variant without a trigger described in FIG. 5 applies here as well.

Step 13. User B loads the main EPC web page providing authentication credentials either entered explicitly or automatically supplied by the web browser.

Step 14. Recognizing User B as subscriber, the EPC Application invokes a ListCalls web service on the Call Tracking Application querying for calls currently in progress that involve user B. If the optional step of having the EPC Application register for call teardown event when processing user A has been carried out, this registration step is no longer necessary for user B.

Step 15. The EPC Application returns user B's personal web page including the description of the phone call with user A and the "enhance call" button. It may look identical to the web page user A received or it may additionally contain information that user A is already waiting for user B in a data collaboration conference.

Steps 16. User B clicks the "enhance call" button generating an HTTP POST message to the EPC Application.

Step 17. The EPC Application returns confirmation web page with the "enter conference" button and invisible information including the Data Collaboration Application network

## US RE42,883 E

11

address, the conference ID corresponding to the already created data conference and user B's full name to serve as conference participant identifier.

Step 18. User B clicks the "enter conference" button generating HTTP POST to the Data Collaboration Application with conference ID and user B name in it.

Step 19. The Data Collaboration Application returns Data Collaboration-specific content including active content that loads into user B's browser realizing participation in a data conference.

After the data conference is created, the EPC service may optionally provide automated stopping of the data conference when the telephone call is hung up. This is an optional feature depending on the following considerations. The Data Collaboration Application may not expose the external interface for stopping a conference (i.e. it can only be stopped on explicit request from one of the conference participants or automatically when all participants leave). The users may actually prefer to continue data collaboration after the phone call is hung up (e.g. the phone call is used to "ignite" a network gaming session during which no further phone connection is desired by the users).

FIG. 7 shows a call flow for a scenario according to the present invention that provides for automated stopping of the data collaboration conference.

Step 1. User A hangs up the telephone call.

Step 2. The switch hangs up call.

Step 3. The switch reports call teardown event to the Call Tracking Application. In the case of IN PSTN network, this may involve a Parlay interface implemented by the ISCP node.

Step 4. The Call Tracking Application reports the event to the EPC Application by invoking its appropriate web service specified when subscribing for such notification during data conference setup.

Step 5. The EPC Application invokes a web service implemented by the Data Collaboration Application requesting stopping of the data conference associated with the telephone call.

Steps 6-7. The Data Collaboration Application performs its own specific actions for stopping the data conference on user A's and user B's PCs.

The above flows describe scenarios where there is full telephone integration. In the following flows, full telephony integration is not possible (e.g. the PBX does not have required CTI module installed necessary for interfacing with CTI apps such as the EPC service). This reduces the amount of automation that can be included in the EPC service, and requires that users enter the information identifying the call. However, the service is still beneficial to the users by offering simple and widespread addressing based on telephone numbers the users already know in order to create a common meeting space in the form of a data collaboration conference.

Other than the need to have the user enter a telephone number, the service operates in the same way as in the full telephony integration case. Therefore, it is possible to implement the service efficiently to target both types of environments, i.e. one and two subscribers. In addition, the "look and feel" and ergonomics of the service for the users is very similar making it easy to use the service when "switching" between full and limited telephony integration.

FIG. 8 shows a call flow for a scenario according to the present invention wherein a subscriber and non-subscriber are collaborating but do not have access to full telephony integration. The subscriber creates a data conference and identifies it by the non-subscribing user's telephone number. The non-subscribing user needs to enter that telephone num-

12

ber in order to join. The subscriber may be billed for the enhanced service and therefore is in control of creating as well as stopping the data conference. Otherwise the service executes in the same way as in the full telephony integration case. It is noted that the non-subscriber's experience and corresponding part of the flow is exactly the same as in the case of full telephony integration with only one subscriber.

Steps 1-2. A phone call is established between user A, the subscriber, and user B, not a subscriber.

Step 3. During the telephone call, both parties agree to enhance the call with data collaboration. User A, the EPC subscriber, loads the EPC web page into a browser following either explicit or automated (remembered by the browser) authentication.

Step 4. Recognizing user A as a subscriber, the EPC Application returns a personalized web page containing a call enhancement area. In this area user A may enter a telephone number of other parties that user A is on a call with.

Step 5. User A enters user B's telephone number, TN\_B, and clicks the "enhance call" button. This generates an HTTP POST message to the EPC Application transmitting the TN\_B.

Step 6. As an optional step, the EPC Application creates a new instance of data collaboration conference by invoking an appropriate web service exposed by the Data Collaboration Application. As a result, a conference ID is established. This step may not be required if the Data Collaboration Application creates a new instance automatically when the first conference participant joins.

Step 7. The EPC Application returns a confirmation page to user A with the "enter conference" button together with associated information consisting of the Data Collaboration Application network address, the conference ID established in step 6 and user A's full name to be used as a conference participant identifier. Only the "enter conference" button is rendered visibly to the user, the rest of the information is hidden.

Step 8. User A clicks the "enter conference" button which generates an HTTP POST message directly to the Data Collaboration Application with enough information to allow user A's participation in the data collaboration conference.

Step 9. The Data Collaboration Application returns Data Collaboration-specific content including active content that loads into user A's browser realizing participation in a data conference.

Steps 10-15. When user A's participation in data conference is completed, user A informs user B over the telephone call that user B may enter the conference via the main EPC web page. The steps are identical to the corresponding steps 13-18 in the case of full telephony integration with only one subscriber, as described in FIG. 4.

In a further embodiment according to the present invention, steps 8-12 of the above flow can be optimized and performed in a single HTTP Reply cycle.

FIG. 9 shows a call flow for a scenario according to the present invention wherein two subscribers are collaborating but do not have access to full telephony integration. The experience of the subscriber who first initiates call enhancement (and may be billed for it) stays the same as in the previous case described in FIG. 8. The experience of the other subscriber who follows second in enhancing the call side could be further automated by the fact that the EPC service knows that user and may remember the subscribers telephone number. In this case the user will be offered the "enhance call" button immediately after entering a personal EPC web page.



## US RE42,883 E

13

Steps 1-9. After the phone call is established, user A enhances the call. These steps are identical to the corresponding steps in the flow described in FIG. 8.

Step 10. User B loads the main EPC web page providing authentication credentials either entered explicitly or automatically supplied by the browser.

Step 11. The EPC Application remembers user B's telephone number TN\_B, so it does not need to ask for it again. Therefore the reply contains user B's personal web page with the call information and the "enhance call" button. The page could also offer a way to enter and optionally remember an alternative telephone number that may currently be used by user B.

Steps 12-15. User B clicks the "enhance call" button and is taken into a data collaboration conference. These steps are identical to the corresponding steps 16-19 in the full telephony integration flow described in FIG. 6.

Security is an important consideration for any phone or data sharing system. One security concern is the prevention of unauthorized person from snooping the data traffic including media and signaling associated with the data collaboration conference between the valid users. As noted above, the EPC service may rely on HTTPS for securing its own signalling and on similar features implemented by the data collaboration service.

Another security concern is providing assurance to a valid service subscriber that the other data conference participant does not impersonate a valid user participating in the phone call. The EPC service according to the present invention provides such assurance. In particular, the case of full telephony integration and both users subscribing to the service, user A is assured by the EPC service that the person who could participate in the data conference enhancement must be authenticated as the subscriber to the EPC service corresponding to the telephone number user A is on the call with. This provides tight coupling between the person having access to the telephone line and the EPC service account. The EPC service provides information to both users on the subscription status of the other party (subscriber or not).

Additionally, if user A knows user B already and can recognize user B's voice, the user A knows that the person on the other line is user B and also knows that the person joining the data conference can prove to the EPC service that he is indeed user B.

In case of full telephony integration with only one subscriber, user B (non-subscriber) could similarly be assured that the data conference participant is indeed user A. This is because the EPC service tells user B that the other party is a subscriber and has been authenticated as user A. The subscribing user, user A, knows that the person joining the data conference satisfies the following two conditions: knows the telephone number TN\_B of user B and additionally knows exactly the time window when the call is in progress. Furthermore, if an impersonator tries to join the conference after the valid user B joins, both users quickly see that this happens by being informed by the EPC service of a third participant. User A and user B can then quickly terminate the conference. This could still be a disadvantage in that the impersonator may have a short access to sensitive data material. In a separate embodiment according to the present invention, the Data Collaboration Application can be configured to admit a set number of participants in the conference (e.g. for the example above, 2 participants). The conference size limitation leaves an impersonator with a very small time window to join a data conference; i.e. after user A but before user B. If this restriction is still not satisfactory, an optional and additional pass code could be assigned to the conference by one of the users

14

and then exchanged with the other user in the telephone conversation. The other user would be required to enter the pass code in addition to the telephone number prior to joining the data conference.

When only limited telephony integration is available, the same security features as described above based on the knowledge of the telephone number, time window, and optional pass code are applicable.

In addition, the automated conference stopping following teardown of the telephone call feature provides an extra security feature by assuring that the data conference is definitely over once the call ends without requiring any other action.

The security features can be provided as an option in the EPC service. In the event that the users do not want to take the extra steps of providing security, (e.g. setting up and exchanging of a pass code in a non-subscriber case), then the EPC service can offer a simpler, quicker, "single click" usage.

Since the majority of telephone calls are two-party calls, we focused our description so far on that case as noted above. However, the EPC service can easily support multiparty telephone calls.

In the case of full telephony integration, the telephone network can provide information about multiparty calls, i.e. call established, party added/removed, call ended (similarly to two-party call information described above). Further, the Data Collaboration Application must be able to accommodate multiparty conferences.

The EPC service provides an easy means to create data collaboration with a high degree of spontaneity. For example, a two party collaboration that evolves into a 3-way collaboration can be easily handled by the EPC service according to the present invention, by addition of the third party in the middle of the call.

In the event that the third or N-th call leg of the multiparty call is the only subscriber, the EPC service of the present invention is still useful. In particular, upon the N-th call leg (subscriber) being established, the subscriber may use the EPC service in a way similar to that described above. The EPC Application will show the subscriber the multiparty call information (including information about all parties) and an "enhance call" button next to it. Further, if the N-th caller is not a subscriber, then such caller, may enter a collaboration session, in the same fashion as described above for a non-subscriber.

In the case of limited telephony integration, the two-party call scenarios are easily extended to multi-party by requiring the subscriber to enter the telephone number(s) of non-subscriber(s). The EPC Application supplies the same data conference ID to the browsers/apps of all users participating in a multi-party telephone call and thus ensures that they all land in the same instance of the data conference. Participant information is provided by the EPC service as well in the form of names and telephone numbers and represented accordingly in the multi-party data conference.

It is anticipated that other embodiments and variations of the present invention will be readily apparent to the skilled artisan in the light of the foregoing description and examples, and it is intended that such embodiments and variations likewise be included within the scope of the invention as set out in the appended claims.

What is claimed is:

1. A method for transitioning from an existing telephone call to a real-time collaboration session in a system including a telephone network for establishing connections between users and a data network for establishing data sharing sessions between said users, each of said users having an associated user access and presentation device, said data network

## US RE42,883 E

15

including an enhanced phone based collaboration (EPC) application, and at least one of said users subscribing to said enhanced phone based *collaboration* application, said method [including the step of] *comprising*:

*responsive to* said one user on an existing telephone call [user] *clicking on a control button on said user's associated device, a server in a telephone network* invoking the operation of said EPC application [solely by clicking on a control button on said user's associated device] to cause said enhanced phone based collaboration to add the collaboration session to the existing telephone call between said users without the users exchanging collaboration session [identifiers] *identifiers*.

2. The method of claim 1 [for transitioning from an existing telephone call to a real time collaboration session], wherein said user access and presentation device is a PC, a notepad, or a PDA.

3. The method of claim 1 [for transitioning from an existing telephone call to a real time collaboration session], wherein said one of said users subscribes to said enhanced phone based collaboration application [but], *and wherein* at least another of said users is a guest non-subscribing user, said method further comprising [the steps of]:

*responsive to* said one subscribing user providing a guest page Uniform Resource Location (URL) for the guest non-subscribing user [said server in a telephone network] *permitting* said guest user using the URL to open a web page to gain access to the enhanced *phone* based collaboration application; and

*enabling* said guest user [entering] *to enter* the real-time collaboration session by entering [its own] a telephone number and clicking on an "enter conference" button on said guest user's associated device.

4. The method of claim 3 [for transitioning from an existing telephone call to a real time collaboration session], wherein said web page is in a browser.

5. The method of claim 3 [for transitioning from an existing telephone call to a real time collaboration session], wherein said session includes a plurality of guest non-subscribing users, each of said plurality of guest non-subscribing users gaining access to the enhanced phone based collaboration application and entering the session by [its own] a telephone number and clicking on [an "enter conference button"] a control button on [its associated] *said device associated with said guest user*.

6. A method for [transition] *transitioning* an existing telephone call to a real-time collaboration session in a system including a telephone network for establishing telephone connections between users and a data network for establishing data sharing sessions between each of said users, each of said users having an associated user access and presentation device, said data network including an enhanced phone based

16

collaboration (EPC) application, and at least one of said users subscribing to said enhanced phone based collaboration application, and said *at least* one user having a plurality of telephone calls in progress, said method comprising [the steps of]:

tracking the in progress telephone calls of said *at least* one user; [and]

choosing a particular one of said telephone calls in progress to be transitioned to the real-time collaboration session [and]; and

said *at least* one user clicking on a control button on said [user's associated] device *associated with said at least one user* to cause said enhanced based phone collaboration application to add the collaboration session to the chosen [existing] telephone call.

7. The method of claim 6 [for transitioning from an existing telephone call to a real-time collaboration session], wherein said tracking [step] comprises displaying to said one user a list of the in progress telephone calls over a web interface and said [step of] choosing comprises said one user clicking on an established telephone call on said list.

8. The method of claim 1 [for transitioning from an existing telephone call to a real-time collaboration session], wherein at least two of the users to be transitioned to the real-time collaboration session subscribe to the enhanced [based phone] *phone based* collaboration application, said method further [comprises] comprising [the step of]

[each of said two subscribing users selecting the telephone call to be enhanced; and]

[each of said two subscribing users] adding the collaboration session to the existing telephone call [simply by] *responsive to each of two subscriber users* clicking on an ["enhanced call"] *"enhance call"* button on [its] *the respective* associated device.

9. The method of claim 1 [for transitioning from an existing telephone call to a real-time collaboration session], wherein one of said users subscribes to said enhanced phone based collaboration application [but], *and wherein* a second of said [subscribers] *users* is a guest non-subscribing user, said enhanced based phone collaboration application including a choice driven web page, said method further comprising [the steps of]

*enabling* said one user [loading] *to load* an EPC web page into a browser [and];

after said one user has clicked on said one user's "enter conference" button, said one user advising said guest user that the guest user may enter the collaboration session via the EPC web page; and

said guest users entering the collaboration session using its own telephone number and an "enter conference button" on its associated device].

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : RE42,883 E  
APPLICATION NO. : 12/001975  
DATED : November 1, 2011  
INVENTOR(S) : Korycki et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title page, item (56), under "Other Publications", Lines 1-2, delete "International Search Report for PCT Pat. App. No. PCT/US04/21407, mailed Dec. 7, 2004." and insert -- International Search Report for PCT Pat. App. No. PCT/US04/21407, mailed Dec. 7, 2004.  
International Preliminary Examination Report for PCT Pat. App. No. PCT/US04/21407, completed May 18, 2005. --.

Column 16, line 13, in Claim 6, delete "based phone" and insert -- phone based --.

Column 16, line 40, in Claim 9, delete "based phone" and insert -- phone based --.

Signed and Sealed this  
Nineteenth Day of June, 2012

A handwritten signature in dark ink, reading "David J. Kappos". The signature is written in a cursive, flowing style with a large initial "D" and a stylized "K".

David J. Kappos  
*Director of the United States Patent and Trademark Office*

# Exhibit U

---

**PATENT ASSIGNMENT COVER SHEET**Electronic Version v1.1  
Stylesheet Version v1.2

EPAS ID: PAT5892380

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT	
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT	
<b>CONVEYING PARTY DATA</b>		
<b>Name</b>		<b>Execution Date</b>
INTELLECTUAL VENTURES ASSETS 130 LLC		11/15/2019
<b>RECEIVING PARTY DATA</b>		
<b>Name:</b>	COMMWORKS SOLUTIONS, LLC	
<b>Street Address:</b>	44 MILTON AVENUE	
<b>Internal Address:</b>	SUITE 254	
<b>City:</b>	ALPHARETTA	
<b>State/Country:</b>	GEORGIA	
<b>Postal Code:</b>	30009	
<b>PROPERTY NUMBERS Total: 66</b>		
<b>Property Type</b>	<b>Number</b>	
Patent Number:	6721787	
Patent Number:	6917605	
Patent Number:	8160863	
Patent Number:	7835897	
Patent Number:	RE42227	
Patent Number:	8195442	
Patent Number:	8380481	
Patent Number:	7069483	
Patent Number:	7852796	
Patent Number:	7835372	
Patent Number:	7451365	
Patent Number:	7957356	
Patent Number:	7941149	
Patent Number:	8175613	
Patent Number:	8780770	
Patent Number:	8611320	
Patent Number:	9554304	
Patent Number:	9930575	
Patent Number:	7092986	

Property Type	Number
Patent Number:	RE43704
Patent Number:	7760664
Patent Number:	6836466
Patent Number:	6775253
Patent Number:	6628943
Patent Number:	6788660
Patent Number:	6487406
Patent Number:	6490259
Patent Number:	RE42883
Patent Number:	6985724
Patent Number:	6857007
Patent Number:	8224909
Patent Number:	8533278
Patent Number:	6891807
Patent Number:	7177285
Patent Number:	7463596
Patent Number:	7911979
Patent Number:	7051116
Patent Number:	7484005
Patent Number:	7814230
Patent Number:	6775258
Patent Number:	6865237
Patent Number:	7006579
Patent Number:	8031800
Patent Number:	7460609
Patent Number:	7355961
Patent Number:	RE43746
Patent Number:	7061379
Patent Number:	6724883
Patent Number:	6594356
Patent Number:	7027465
Patent Number:	RE44904
Patent Number:	7209950
Patent Number:	7224642
Patent Number:	6980089
Patent Number:	7245201
Patent Number:	7248148
Patent Number:	6956941

Property Type	Number
Patent Number:	6859529
Patent Number:	6456764
Patent Number:	6804713
Patent Number:	6335821
Patent Number:	6483634
Patent Number:	6427037
Patent Number:	6901437
Patent Number:	9648122
Patent Number:	10051077

**CORRESPONDENCE DATA**

**Fax Number:** (404)645-7707

*Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.*

**Phone:** 4046457700

**Email:** docketing@mcciplaw.com

**Correspondent Name:** LAWRENCE AARONSON

**Address Line 1:** 999 PEACHTREE STREET NE

**Address Line 2:** SUITE 1300

**Address Line 4:** ATLANTA, GEORGIA 30309

<b>ATTORNEY DOCKET NUMBER:</b>	11201-001GEN
<b>NAME OF SUBMITTER:</b>	LAWRENCE A. AARONSON
<b>SIGNATURE:</b>	/Lawrence A. Aaronson/
<b>DATE SIGNED:</b>	01/03/2020

**Total Attachments: 11**

source=IV 130 to CommWorks Solutions (Active)#page1.tif  
source=IV 130 to CommWorks Solutions (Active)#page2.tif  
source=IV 130 to CommWorks Solutions (Active)#page3.tif  
source=IV 130 to CommWorks Solutions (Active)#page4.tif  
source=IV 130 to CommWorks Solutions (Active)#page5.tif  
source=IV 130 to CommWorks Solutions (Active)#page6.tif  
source=IV 130 to CommWorks Solutions (Active)#page7.tif  
source=IV 130 to CommWorks Solutions (Active)#page8.tif  
source=IV 130 to CommWorks Solutions (Active)#page9.tif  
source=IV 130 to CommWorks Solutions (Active)#page10.tif  
source=IV 130 to CommWorks Solutions (Active)#page11.tif



**Exhibit A-2****ASSIGNMENT OF PATENT RIGHTS**

For good and valuable consideration, the receipt of which is hereby acknowledged, Intellectual Ventures Assets 130 LLC, a Delaware limited liability company, with an address at 251 Little Falls Drive, Wilmington, DE 19808 ("**Assignor**"), does hereby sell, assign, transfer, and convey unto CommWorks Solutions, LLC, a Georgia limited liability company with an address at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009 ("**Assignee**"), all of Assignor's right, title, and interest in and to the following (collectively, the "**Assigned Patent Rights**"):

(a) the patents and patent applications listed in the table below (the "**Patents**");

**Active Patent(s) – (Filed; Granted)**

<b>Patent/Application Number</b>	<b>Country</b>	<b>Issue Date/ Filing Date</b>	<b>Title of Patent and First Named Inventor</b>
6721787  (09/501204)	US	4/13/2004  (2/10/2000)	SYSTEM AND METHOD FOR WIRELESS HOT- SYNCHRONIZATION OF A PERSONAL DIGITAL ASSISTANT  James Scott Hiscock
JP4294829  (JP2000-125968)	JP	4/17/2009  (4/26/2000)	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION REVISION METHOD  KAKEMIZU MITSUAKI
DE60121094.8  (DE60121094.8)	DE	6/28/2006  (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
FR1150530  (FR01102111.0)	FR	6/28/2006  (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
GB1150530  (GB01102111.0)	GB	6/28/2006  (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
6917605  (09/770019)	US	7/12/2005  (1/25/2001)	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION CHANGING METHOD  Kakemizu, Mitsuaki

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
8160863 (10/044217)	US	4/17/2012 (11/19/2001)	System and method for connecting a logic circuit simulation to a network  Robert M. Zeidman
7835897 (11/557064)	US	11/16/2010 (11/6/2006)	APPARATUS AND METHOD FOR CONNECTING HARDWARE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
RE42227 (12/481943)	US	3/15/2011 (6/10/2009)	Apparatus and method for connecting hardware to a circuit simulation  Robert Marc Zeidman
8195442 (12/946721)	US	6/5/2012 (11/15/2010)	APPARATUS AND METHOD FOR CONNECTING HARDWARE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
8380481 (13/487750)	US	2/19/2013 (6/4/2012)	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
7069483 (10/437128)	US	6/27/2006 (5/13/2003)	System and method for identifying nodes in a wireless mesh network  Michael P. Nova
JP4874550 (JP2004-572210)	JP	12/2/2011 (10/31/2003)	System and method for routing packets in a wired or wireless network  GILLIES DONALD W
JP4369374 (JP2004-572211)	JP	11/18/2009 (10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  WANG WEILIN

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7852796 (11/420668)	US	12/14/2010 (5/26/2006)	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION  Xudong Wang
7835372 (11/421998)	US	11/16/2010 (6/2/2006)	System and Method for Transparent Wireless Bridging of Communication Channel Segments  Weilin Wang
7451365 (11/425114)	US	11/11/2008 (6/19/2006)	System and Method for Identifying Nodes in a Wireless Network  Donald W. Gillies
7957356 (11/462663)	US	6/7/2011 (8/4/2006)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI- HOP HIGH BANDWIDTH COMMUNICATIONS  Xudong Wang
7941149 (11/615582)	US	5/10/2011 (12/22/2006)	Multi-Hop Ultra Wide Band Wireless Network Communication  Weilin Wang
8175613 (11/741630)	US	5/8/2012 (4/27/2007)	SYSTEMS AND METHODS FOR DETERMINING LOCATION OF DEVICES WITHIN A WIRELESS NETWORK  Chao Gui
8780770 (11/741637)	US	7/15/2014 (4/27/2007)	SYSTEMS AND METHODS FOR VOICE COMMUNICATION OVER A WIRELESS NETWORK  Weiguang Shi
8611320 (12/950558)	US	12/17/2013 (11/19/2010)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS

<b>Patent/Application Number</b>	<b>Country</b>	<b>Issue Date/ Filing Date</b>	<b>Title of Patent and First Named Inventor</b>
			Weilin Wang
9554304 (14/090760)	US	1/24/2017 (11/26/2013)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Xudong Wang
9930575 (15/409896)	US	3/27/2018 (1/19/2017)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Weilin Wang
7092986 (10/067278)	US	8/15/2006 (2/7/2002)	Transparent mobile IPv6 agent  Wang, Mei Na
RE43704 (12/608732)	US	10/2/2012 (10/29/2009)	Determining and provisioning paths within a network of communication elements  Gupta, Sanyogita
7760664 (11/101136)	US	7/20/2010 (4/7/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
CA2581734 (CA2581734)	CA	8/28/2012 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
DE602005053126.2 (DE602005053126.2)	DE	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
GB1797670 (GB05857725.5)	GB	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
JP4777990 (JP2007-534687)	JP	7/8/2011 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
6836466 (09/579371)	US	12/28/2004 (5/26/2000)	Method and system for measuring IP performance metrics  Krishna Kant
6775253 (09/512644)	US	8/10/2004 (2/24/2000)	Adaptive signaling for wireless packet telephony  Prathima Agrawal
6628943 (09/512645)	US	9/30/2003 (2/24/2000)	Mobility management utilizing active address propagation  Prathima Agrawal
6788660 (09/512646)	US	9/7/2004 (2/24/2000)	Adaptive mobile signaling for wireless internet telephony  Prathima Agrawal
6487406 (09/545619)	US	11/26/2002 (4/10/2000)	PCS-to-mobile IP internetworking  Li-Fung Chang
TWI183532 (TW089110383)	TW	8/11/2003 (5/29/2000)	PCS-to-mobile IP internetworking  Chang, Li-Fung
CA2310783 (CA2310783)	CA	2/3/2004 (6/6/2000)	PCS-to-mobile IP internetworking  Chang, Li-Fung
6490259 (09/512514)	US	12/3/2002 (2/24/2000)	Active link layer and intra- domain mobility for IP networks  AGRAWAL PRATHIMA
RE42883 (12/001975)	US	11/1/2011 (12/13/2007)	Enhanced Phone-Based Collaboration  Korycki, Jacek
6985724 (10/239763)	US	1/10/2006 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno

<b>Patent/Application Number</b>	<b>Country</b>	<b>Issue Date/ Filing Date</b>	<b>Title of Patent and First Named Inventor</b>
6857007 (09/723349)	US	2/15/2005 (11/27/2000)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
8224909 (12/369785)	US	7/17/2012 (2/12/2009)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
8533278 (13/490403)	US	9/10/2013 (6/6/2012)	Mobile computing device based communication systems and methods  Mark C. Bloomfield
6891807 (10/341847)	US	5/10/2005 (1/13/2003)	Time based wireless access provisioning  Roskind, James A.
7177285 (10/961959)	US	2/13/2007 (10/8/2004)	Time based wireless access provisioning  Roskind, James A.
7463596 (11/673513)	US	12/9/2008 (2/9/2007)	TIME BASED WIRELESS ACCESS PROVISIONING  Roskind, James A.
7911979 (12/323399)	US	3/22/2011 (11/25/2008)	Time Based Access Provisioning System and Process  James A. Roskind
7051116 (09/983042)	US	5/23/2006 (10/22/2001)	Client device identification when communicating through a network address translator device  Rodriguez-Val, Richard
7484005 (11/351116)	US	1/27/2009 (2/10/2006)	Client device identification when communicating through a network address translator device  Richard Rodriguez-Val

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7814230 (12/337854)	US	10/12/2010 (12/18/2008)	Client device identification when communicating through a network address translator device  Rodriguez-Val, Richard
6775258 (09/527786)	US	8/10/2004 (3/17/2000)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system  Van Valkenburg, Sander
6865237 (09/676373)	US	3/8/2005 (9/29/2000)	Method and system for digital signal transmission  Boariu, Adrian
7006579 (10/023924)	US	2/28/2006 (12/18/2001)	ISI-robust slot formats for non-orthogonal-based space- time block codes  Kuchi, Kiran
DE60123282.8 (DE01273305.1)	DE	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
GB1350354 (GB01273305.1)	GB	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
8031800 (10/450997)	US	10/4/2011 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
DE60244331.8 (DE60244331.8)	DE	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav
FR1405453 (FR02743313.5)	FR	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav
GB1405453 (GB02743313.5)	GB	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav
7460609 (10/739017)	US	12/2/2008 (12/19/2003)	Transmission method using complex channel symbols  Tirkkonen, Olav



<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7355961 (11/070624)	US	4/8/2008 (3/2/2005)	Method and arrangement for digital signal transmission using layered space-time codes  Tirkkonen, Olav
RE43746 (13/166702)	US	10/16/2012 (6/22/2011)	Method and radio system for digital signal transmission using complex space-time codes  Tirkkonen, Olav
7061379 (10/301846)	US	6/13/2006 (11/21/2002)	RFID system and method for ensuring safety of hazardous or dangerous substances  Chen, Fung-Jou
6724883 (09/660133)	US	4/20/2004 (9/12/2000)	Processing of data message in a network element of a communications network  Lehtinen, Pekka
CNZL00808958.2 (CN00808958.2)	CN	11/10/2004 (6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
DE60042650.5 (DE60042650.5)	DE	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
ES1192811 (ES00942154.6)	ES	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
GB1192811 (GB00942154.6)	GB	7/29/2009 (6/13/2000)	Call set-up control in an intelligent network by conditional initiation of more

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			than one controlling service  Tuunanen, Heikki
IT1192811 (IT00942154.6)	IT	7/29/2009 (6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
6594356 (10/014918)	US	7/15/2003 (12/14/2001)	Initiating a controlling service  Tuunanen, Heikki
7027465 (10/167986)	US	4/11/2006 (6/11/2002)	Method for contention free traffic detection  Hautala Petri
RE44904 (13/171882)	US	5/20/2014 (6/29/2011)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
7209950 (09/921167)	US	4/24/2007 (8/2/2001)	Method and apparatus for a network independent short message delivery system  Simon Bennett
7224642 (11/340733)	US	5/29/2007 (1/26/2006)	Wireless sensor data processing systems  Bao Q. Tran
6980089 (09/924730)	US	12/27/2005 (8/8/2001)	Non-intrusive coupling to shielded power cable  Paul A. Kline
7245201 (10/947929)	US	7/17/2007 (9/23/2004)	Power line coupling device and method of using the same  Paul A. Kline
7248148 (11/265230)	US	7/24/2007 (11/3/2005)	Power line coupling device and method of using the same  Paul A. Kline
6956941 (09/547627)	US	10/18/2005 (4/12/2000)	METHOD AND SYSTEM FOR SCHEDULING INBOUND INQUIRIES  Daniel N. Duncan

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
6859529 (10/082386)	US	2/22/2005 (2/25/2002)	Method and system for self-service scheduling of inbound inquiries  Daniel N. Duncan
6456764 (09/668372)	US	9/24/2002 (9/25/2000)	Optical directional coupler  Hideaki Okayama
6804713 (09/549687)	US	10/12/2004 (4/14/2000)	Operational supervisory system for a server  Miwa Nishio
6335821 (09/501606)	US	1/1/2002 (2/10/2000)	Optical fiber amplifier and a method for controlling the same  Mikiya Suzuki
6483634 (09/662904)	US	11/19/2002 (9/15/2000)	Optical amplifier  Andrew R Pratt
6427037 (09/497235)	US	7/30/2002 (2/3/2000)	Two-stage optical switch circuit network  Hideaki Okayama
6901437 (09/684047)	US	5/31/2005 (10/6/2000)	Mobile cache for dynamically composing user-specific information  Benjamin Bin Li
9648122 (11/133755)	US	5/9/2017 (5/19/2005)	Mobile cache for dynamically composing user-specific information  Benjamin Bin Li
10051077 (15/486546)	US	8/14/2018 (4/13/2017)	Mobile cache for dynamically composing user-specific information  Benjamin Bin Li

(b) any future reissues, reexaminations, extensions, continuations, continuing prosecution application, requests for continuing examinations, divisions, and registrations of any of the Patents;

(c) rights to apply in any or all countries of the world for future patents, certificates of invention, utility models, industrial design protections, design patent protections, or other future governmental grants or issuances of any type related to the Patents; and

(d) causes of action and enforcement rights of any kind under, or on account of, any of the Patents and/or any of the items described in either of the foregoing categories (b) or (c), including, without limitation, all causes of action, enforcement rights and all other rights to seek and obtain any other remedies of any kind for past, current and future infringement.

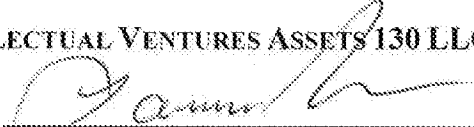
Assignor hereby authorizes the respective patent office or governmental agency in each jurisdiction to issue any and all future patents, certificates of invention, utility models or other governmental grants or issuances that may be granted upon any of the Assigned Patent Rights in the name of Assignee, as the assignee to the entire interest therein. This Assignment of Patent Rights will inure for the benefit of any permitted successors or assigns of Assignee.

Assignor will, at the reasonable request of Assignee, take all reasonable steps necessary and proper, to confirm the assignment to Assignee of the Assigned Patent Rights pursuant to this Assignment of Patent Rights, including without limitation, the execution, acknowledgment, and recordation of specific assignments, oaths, declarations, and other documents on a country-by-country basis, to assist Assignee in obtaining and perfecting the Assigned Patent Rights.

IN WITNESS WHEREOF this Assignment of Patent Rights is executed on November 15, 2019, to be effective as of November 15, 2019.

**ASSIGNOR:**

**INTELLECTUAL VENTURES ASSETS 130 LLC**

By:   
Name: Lawrence Froeber  
Title: CFO

# Exhibit V

---

**PATENT ASSIGNMENT COVER SHEET**Electronic Version v1.1  
Stylesheet Version v1.2

EPAS ID: PAT5892419

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT	
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT	
<b>CONVEYING PARTY DATA</b>		
<b>Name</b>		<b>Execution Date</b>
INTELLECTUAL VENTURES ASSETS 135 LLC		11/15/2019
<b>RECEIVING PARTY DATA</b>		
<b>Name:</b>	COMMWORKS SOLUTIONS, LLC	
<b>Street Address:</b>	44 MILTON AVENUE	
<b>Internal Address:</b>	SUITE 254	
<b>City:</b>	ALPHARETTA	
<b>State/Country:</b>	GEORGIA	
<b>Postal Code:</b>	30009	
<b>PROPERTY NUMBERS Total: 72</b>		
<b>Property Type</b>	<b>Number</b>	
Patent Number:	6832249	
Patent Number:	8423630	
Patent Number:	8812665	
Patent Number:	6621854	
Patent Number:	6711122	
Patent Number:	7180850	
Patent Number:	7564863	
Patent Number:	7626918	
Patent Number:	7609712	
Patent Number:	7062475	
Patent Number:	7596533	
Patent Number:	RE42232	
Patent Number:	6931003	
Patent Number:	7835350	
Patent Number:	RE43163	
Patent Number:	7079823	
Patent Number:	6490067	
Patent Number:	6748064	
Patent Number:	6636742	

Property Type	Number
Patent Number:	6868268
Patent Number:	RE42539
Patent Number:	8117068
Patent Number:	7412514
Patent Number:	7734807
Patent Number:	8671216
Patent Number:	6771971
Patent Number:	7206806
Patent Number:	6866587
Patent Number:	6427001
Patent Number:	6505163
Patent Number:	6721415
Patent Number:	7023978
Patent Number:	6795530
Patent Number:	RE42122
Patent Number:	6792094
Patent Number:	6754323
Patent Number:	7363030
Patent Number:	6967951
Patent Number:	7856011
Patent Number:	8107377
Patent Number:	8913618
Patent Number:	6785534
Patent Number:	6754716
Patent Number:	6678080
Patent Number:	7937081
Patent Number:	8200211
Patent Number:	8351924
Patent Number:	8600372
Patent Number:	8923846
Patent Number:	9432842
Patent Number:	9918222
Patent Number:	6665495
Patent Number:	7145867
Patent Number:	7184444
Patent Number:	7526203
Patent Number:	7443790
Patent Number:	8116315



Property Type	Number
Patent Number:	7106697
Patent Number:	7218637
Patent Number:	7190900
Patent Number:	7474853
Patent Number:	7496033
Patent Number:	7869427
Patent Number:	7715712
Patent Number:	7124435
Patent Number:	7254709
Patent Number:	8719326
Patent Number:	9230039
Patent Number:	6456242
Patent Number:	6433742
Patent Number:	6456245
Patent Number:	6438367

**CORRESPONDENCE DATA**

**Fax Number:** (404)645-7707

*Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.*

**Phone:** 4046457700

**Email:** docketing@mcciplaw.com

**Correspondent Name:** LAWRENCE AARONSON

**Address Line 1:** 999 PEACHTREE STREET NE

**Address Line 2:** SUITE 1300

**Address Line 4:** ATLANTA, GEORGIA 30309

<b>ATTORNEY DOCKET NUMBER:</b>	11201-001GEN
<b>NAME OF SUBMITTER:</b>	LAWRENCE A. AARONSON
<b>SIGNATURE:</b>	/Lawrence A. Aaronson/
<b>DATE SIGNED:</b>	01/03/2020

**Total Attachments: 10**

source=IV 135 to CommWorks Solutions (Active)#page1.tif  
source=IV 135 to CommWorks Solutions (Active)#page2.tif  
source=IV 135 to CommWorks Solutions (Active)#page3.tif  
source=IV 135 to CommWorks Solutions (Active)#page4.tif  
source=IV 135 to CommWorks Solutions (Active)#page5.tif  
source=IV 135 to CommWorks Solutions (Active)#page6.tif  
source=IV 135 to CommWorks Solutions (Active)#page7.tif  
source=IV 135 to CommWorks Solutions (Active)#page8.tif  
source=IV 135 to CommWorks Solutions (Active)#page9.tif  
source=IV 135 to CommWorks Solutions (Active)#page10.tif

**Exhibit A-1****ASSIGNMENT OF PATENT RIGHTS**

For good and valuable consideration, the receipt of which is hereby acknowledged, Intellectual Ventures Assets 135 LLC, a Delaware limited liability company, with an address at 251 Little Falls Drive, Wilmington, DE 19808 ("**Assignor**"), does hereby sell, assign, transfer, and convey unto CommWorks Solutions, LLC, a Georgia limited liability company with an address at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009 ("**Assignee**"), all of Assignor's right, title, and interest in and to the following (collectively, the "**Assigned Patent Rights**"):

(a) the patents and patent applications listed in the table below (the "**Patents**");

**Active Patent(s) – (Filed; Granted)**

<b>Patent/Application Number</b>	<b>Country</b>	<b>Issue Date/ Filing Date</b>	<b>Title of Patent and First Named Inventor</b>
6832249 (09/860801)	US	12/14/2004 (5/18/2001)	Globally accessible computer network-based broadband communication system with user-controllable quality of information delivery and flow priority  Cisco, Larry
8423630 (10/978953)	US	4/16/2013 (11/1/2004)	Responding to Quality of Service Events in a Multi-Layered Communication System  Steven Reynolds
8812665 (13/781130)	US	8/19/2014 (2/28/2013)	MONITORING FOR AND RESPONDING TO QUALITY OF SERVICE EVENTS IN A MULTI-LAYERED COMMUNICATION SYSTEM  Cisco, Larry
6621854 (08/003996)	US	9/16/2003 (1/15/1993)	Spread-spectrum electromagnetic signals  Bart F. Rice
6711122 (09/500750)	US	3/23/2004 (2/8/2000)	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION  John B. Langley
7180850 (10/762197)	US	2/20/2007 (1/20/2004)	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION  John B. Langley

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7564863 (11/504144)	US	7/21/2009 (8/14/2006)	Frequency offset differential pulse position modulation  Langley, John B.
7626918 (11/504252)	US	12/1/2009 (8/14/2006)	Frequency offset differential pulse position modulation  Michael Mancusi
7609712 (11/504967)	US	10/27/2009 (8/15/2006)	Frequency offset differential pulse position modulation  Michael Mancusi
7062475 (10/715218)	US	6/13/2006 (11/17/2003)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT  Andrew Szabo
7596533 (11/467888)	US	9/29/2009 (8/28/2006)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT  Seth Elliott
RE42232 (11/376700)	US	3/22/2011 (3/15/2006)	RF chipset architecture  Dominik J. Schmidt
6931003 (09/753743)	US	8/16/2005 (12/27/2000)	PACKET PRIORITIZATION PROTOCOL FOR A LARGE-SCALE, HIGH SPEED COMPUTER NETWORK  Keith R. Anderson
7835350 (11/180764)	US	11/16/2010 (7/13/2005)	PRIORITIZING DATA TRANSMISSIONS USING THE NUMBER OF ASSOCIATED ORIGIN ADDRESSES  Keith R. Anderson
RE43163 (11/318396)	US	2/7/2012 (12/22/2005)	HIGH-SPEED NETWORK OF INDEPENDENTLY LINKED NODES  Keith R. Anderson
7079823 (09/980027)	US	7/18/2006 (2/27/2002)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
			MORCHE, Dominique
6490067 (09/860078)	US	12/3/2002 (5/16/2001)	MULTI-CHANNEL OPTICAL TRANSCIVER  Scott H. Bloom
6748064 (09/749994)	US	6/8/2004 (12/28/2000)	SYSTEMS AND METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
6636742 (09/599201)	US	10/21/2003 (6/22/2000)	TRACKING OF MOBILE TERMINAL EQUIPMENT IN A MOBILE COMMUNICATIONS SYSTEM  TORKKI, Markus
6868268 (09/896835)	US	3/15/2005 (6/29/2001)	AUDIO CALLING NAME AND NUMBER DELIVERY  James A. Worsham
RE42539 (11/727638)	US	7/12/2011 (3/27/2007)	NETWORK AND METHOD FOR PROVIDING A CALLING NAME TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang
8117068 (12/464782)	US	2/14/2012 (5/12/2009)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK  Brian Mark Shuster
7412514 (09/932431)	US	8/12/2008 (8/17/2001)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7734807 (12/189417)	US	6/8/2010 (8/11/2008)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster
8671216 (12/795597)	US	3/11/2014 (6/7/2010)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster
6771971 (09/764696)	US	8/3/2004 (1/18/2001)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC)  Steven W. Smith
7206806 (09/870536)	US	4/17/2007 (5/30/2001)	Method and system for remote utilizing a mobile device to share data objects  Richard A. Pineau
6866587 (09/669479)	US	3/15/2005 (9/25/2000)	WIDE AREA REAL-TIME SOFTWARE ENVIRONMENT  Greg Lane
6427001 (09/874998)	US	7/30/2002 (6/7/2001)	SYSTEM AND METHOD FOR NOTIFICATION OF 911 TELEPHONE CALLS USING LINK MONITORING SYSTEM  Sunil H. Contractor
6505163 (09/634794)	US	1/7/2003 (8/9/2000)	NETWORK AND METHOD FOR PROVIDING AN AUTOMATIC RECALL TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang
6721415 (09/506021)	US	4/13/2004 (2/17/2000)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  Quenton Lanny Gilbert

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7023978  (10/818817)	US	4/4/2006  (4/6/2004)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  Quenton Lanny Gilbert
6795530  (09/606062)	US	9/21/2004  (6/29/2000)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Lanny Gilbert
RE42122  (11/971456)	US	2/8/2011  (1/9/2008)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Raymond J. Smets
6792094  (09/863477)	US	9/14/2004  (5/23/2001)	INTELLIGENT CALL CONNECTION SERVICE  Mark Kirkpatrick
6754323  (10/025722)	US	6/22/2004  (12/19/2001)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  E-Lee Chang
7363030  (10/852528)	US	4/2/2008  (5/24/2004)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  Linda Ann Roberts
6967951  (10/044244)	US	11/22/2005  (1/11/2002)	SYSTEM FOR REORDERING SEQUENCED BASED PACKETS IN A SWITCHING NETWORK  Vic Alfano
7856011  (11/237482)	US	12/21/2010  (9/27/2005)	Reordering packets  Vic Alfano
8107377  (12/759221)	US	1/31/2012  (4/13/2010)	Reordering packets  Vic Alfano

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
8913618 (13/337717)	US	12/16/2014 (12/27/2011)	Reordering packets Vic Alfano
6785534 (09/832011)	US	8/31/2004 (4/11/2001)	PREPAID/POSTPAID AUTOMATIC CHANGE OF PAYMENT OPTION Dara Ung
6754716 (09/502155)	US	6/22/2004 (2/11/2000)	RESTRICTING COMMUNICATION BETWEEN NETWORK DEVICES ON A COMMON NETWORK Rosen Sharma
DE60037651.6 (DE60037651.6)	DE	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
FR1151567 (FR00903718.5)	FR	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
GB1151567 (GB00903718.5)	GB	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
6678080 (09/923845)	US	1/13/2004 (8/7/2001)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
7937081 (12/720862)	US	5/3/2011 (3/10/2010)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8200211 (13/097709)	US	6/12/2012 (4/29/2011)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8351924 (13/484583)	US	1/8/2013 (5/31/2012)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8600372 (13/682230)	US	12/3/2013 (11/20/2012)	RECOVERY TECHNIQUES IN MOBILE NETWORKS



<b>Patent/Application Number</b>	<b>Country</b>	<b>Issue Date/ Filing Date</b>	<b>Title of Patent and First Named Inventor</b>
			Heikki Juhani Einola
8923846 (14/058473)	US	12/30/2014 (10/21/2013)	RECOVERY TECHNIQUES IN MOBILE NETWORKS
			Heikki Juhani Einola
9432842 (14/549714)	US	8/30/2016 (11/21/2014)	RECOVERY TECHNIQUES IN MOBILE NETWORKS
			Heikki Juhani Einola
9918222 (15/226422)	US	3/13/2018 (8/2/2016)	RECOVERY TECHNIQUES IN MOBILE NETWORKS
			Heikki Juhani Einola
6665495 (09/698666)	US	12/16/2003 (10/27/2000)	NON-BLOCKING, SCALABLE OPTICAL ROUTER ARCHITECTURE AND METHOD FOR ROUTING OPTICAL TRAFFIC
			Miles, Larry L.
7145867 (10/114564)	US	12/5/2006 (4/2/2002)	SYSTEM AND METHOD FOR SLOT DEFLECTION ROUTING
			Aicklen, Gregory H.
7184444 (10/138760)	US	2/27/2007 (5/3/2002)	SYSTEM AND METHOD FOR PACKET CLASSIFICATION
			Posey, Nolan J. JR.
7526203 (10/659485)	US	4/28/2009 (9/10/2003)	Apparatus and method for optical switching at an optical switch fabric
			Tamil, Lakshman S.
7443790 (11/368867)	US	10/28/2008 (3/6/2006)	System and method for slot deflection routing at optical router/switch
			Aicklen, Gregory H.
8116315 (11/471149)	US	2/14/2012 (6/20/2006)	SYSTEM AND METHOD FOR PACKET CLASSIFICATION
			Posey, Nolan J. JR.

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7106697 (10/114925)	US	9/12/2006 (4/3/2002)	METHOD FOR DYNAMICALLY COMPUTING A SWITCHING SCHEDULE  Robert E. Best
7218637 (10/114928)	US	5/15/2007 (4/3/2002)	System For Switching Data Using Dynamic Scheduling  Robert E. Best
7190900 (10/063301)	US	3/13/2007 (4/9/2002)	System and method for implementing dynamic scheduling of data in a non- blocking all-optical switching network  Best, Robert E.
7474853 (11/299889)	US	1/6/2009 (12/12/2005)	NON-BLOCKING ALL- OPTICAL SWITCHING NETWORK DYNAMIC DATA SCHEDULING SYSTEM AND IMPLEMENTATION METHOD  Robert Best , Ramaswamy Chandrasekaran
7496033 (11/453755)	US	02/24/2009 (6/15/2006)	Method for dynamically computing a switching schedule  Robert Best
7869427 (11/796682)	US	01/11/2011 (04/27/2007)	SYSTEM FOR SWITCHING DATA USING DYNAMIC SCHEDULING  Robert E. Best
7715712 (12/185198)	US	5/11/2010 (08/04/2008)	SYSTEM AND METHOD FOR IMPLEMENTING DYNAMIC SCHEDULING OF DATA IN A NON-BLOCKING ALL- OPTICAL SWITCHING NETWORK  Robert E. Best
7124435 (10/040933)	US	10/17/2006 (10/23/2001)	Information management system and method  Philippe Richard

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
7254709 (10/699632)	US	8/7/2007 (11/1/2003)	Managed information transmission of electronic items in a network environment  Philippe Richard
8719326 (11/188095)	US	5/6/2014 (7/22/2005)	Adaptive data transformation engine  Philippe Richard
9230039 (14/223936)	US	1/5/2016 (3/24/2014)	Adaptive data transformation engine  Philippe Richard
6456242 (09/799411)	US	9/24/2002 (3/5/2001)	CONFORMAL BOX ANTENNA  James A. Crawford
6433742 (09/693465)	US	8/13/2002 (10/19/2000)	DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS  CRAWFORD JAMES A
6456245 (09/735977)	US	9/24/2002 (12/13/2000)	CARD-BASED DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS  James A. Crawford
6438367 (09/710614)	US	8/20/2002 (11/9/2000)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS  CRAWFORD JAMES A

(b) any future reissues, reexaminations, extensions, continuations, continuing prosecution application, requests for continuing examinations, divisions, and registrations of any of the Patents;

(c) rights to apply in any or all countries of the world for future patents, certificates of invention, utility models, industrial design protections, design patent protections, or other future governmental grants or issuances of any type related to the Patents; and

(d) causes of action and enforcement rights of any kind under, or on account of, any of the Patents and/or any of the items described in either of the foregoing categories (b) or (c), including, without limitation, all causes of action, enforcement rights and all other rights to seek and obtain any other remedies of any kind for past, current and future infringement.

Assignor hereby authorizes the respective patent office or governmental agency in each jurisdiction to issue any and all future patents, certificates of invention, utility models or other governmental grants or issuances that may be granted upon any of the Assigned Patent Rights in the name of Assignee, as the assignee to the entire interest therein. This Assignment of Patent Rights will inure for the benefit of any permitted successors or assigns of Assignee.

Assignor will, at the reasonable request of Assignee, take all reasonable steps necessary and proper, to confirm the assignment to Assignee of the Assigned Patent Rights pursuant to this Assignment of Patent Rights, including without limitation, the execution, acknowledgment, and recordation of specific assignments, oaths, declarations, and other documents on a country-by-country basis, to assist Assignee in obtaining and perfecting the Assigned Patent Rights.

IN WITNESS WHEREOF this Assignment of Patent Rights is executed on November 15, 2019, 2019, to be effective on November 15, 2019.

**ASSIGNOR:**

**INTELLECTUAL VENTURES ASSETS 135 LLC**

By: 

Name: Lawrence Froeber

Title: CFO

# Exhibit W

---

**PATENT ASSIGNMENT COVER SHEET**Electronic Version v1.1  
Stylesheet Version v1.2

EPAS ID: PAT5892440

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT	
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT	
<b>CONVEYING PARTY DATA</b>		
<b>Name</b>		<b>Execution Date</b>
INTELLECTUAL VENTURES ASSETS 135 LLC		11/15/2019
<b>RECEIVING PARTY DATA</b>		
<b>Name:</b>	COMMWORKS SOLUTIONS, LLC	
<b>Street Address:</b>	44 MILTON AVENUE	
<b>Internal Address:</b>	SUITE 254	
<b>City:</b>	ALPHARETTA	
<b>State/Country:</b>	GEORGIA	
<b>Postal Code:</b>	30009	
<b>PROPERTY NUMBERS Total: 46</b>		
<b>Property Type</b>	<b>Number</b>	
Patent Number:	5210770	
Patent Number:	5267271	
Patent Number:	5452328	
Patent Number:	5815526	
Patent Number:	5991333	
Patent Number:	7760792	
Patent Number:	7457345	
Patent Number:	7457348	
Patent Number:	7924906	
Patent Number:	7706247	
Patent Number:	6710424	
Patent Number:	6667967	
Patent Number:	7555273	
Patent Number:	6873686	
Patent Number:	6985561	
Patent Number:	7769374	
Patent Number:	6650616	
Application Number:	12755012	
Application Number:	09584057	

Property Type	Number
Application Number:	11423847
Application Number:	11147853
Application Number:	11514294
Application Number:	10287109
Application Number:	11447279
Application Number:	11256618
Application Number:	11724311
Application Number:	60213827
Application Number:	60213396
Application Number:	60226108
Application Number:	60225943
Application Number:	09893362
Application Number:	13353787
Application Number:	60225888
Application Number:	60190646
Application Number:	09686598
Application Number:	11725192
Application Number:	12046610
Application Number:	60196095
Application Number:	15887481
Application Number:	10063268
Application Number:	60246821
Application Number:	10012240
Application Number:	60403873
Application Number:	60484885
Application Number:	10643734
Application Number:	60590489

**CORRESPONDENCE DATA**

**Fax Number:** (404)645-7707

*Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.*

**Phone:** 4046457700

**Email:** docketing@mcciplaw.com

**Correspondent Name:** LAWRENCE AARONSON

**Address Line 1:** 999 PEACHTREE STREET NE

**Address Line 2:** SUITE 1300

**Address Line 4:** ATLANTA, GEORGIA 30309

**ATTORNEY DOCKET NUMBER:** 11201-001GEN



<b>NAME OF SUBMITTER:</b>	LAWRENCE A. AARONSON
<b>SIGNATURE:</b>	/Lawrence A. Aaronson/
<b>DATE SIGNED:</b>	01/03/2020
<b>Total Attachments: 9</b> source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page1.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page2.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page3.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page4.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page5.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page6.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page7.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page8.tif source=IV 135 to CommWorks Solutions (Lapsed-Expired)#page9.tif	

**Exhibit B-1****ASSIGNMENT OF RIGHTS IN CERTAIN ASSETS**

For good and valuable consideration, the receipt of which is hereby acknowledged, Intellectual Ventures Assets 135 LLC, a Delaware limited liability company, with an address at 251 Little Falls Drive, Wilmington, DE 19808 ("**Assignor**"), does hereby sell, assign, transfer, and convey unto CommWorks Solutions, LLC, a Georgia limited liability company with an address at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009 ("**Assignee**"), its right, title, and interest in and to any and all of the following provisional patent applications, patent applications, patents, and other governmental grants or issuances of any kind (the "**Certain Assets**");

**Inactive Patent(s) – (Abandoned; Lapsed; Expired)**

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
(PCT/US2001/016291)	WO	(5/18/2001)	Globally accessible computer network-based broadband communication system with user-controllable quality of information delivery and flow priority  Ciscon, Larry
5210770 (07/766372)	US	5/11/1993 (9/27/1991)	MULTIPLE-SIGNAL SPREAD-SPECTRUM TRANSCEIVER  Bart F. Rice
5267271 (07/907358)	US	11/30/1993 (7/1/1992)	Signal analysis technique for determining a subject of binary sequences most likely to have been transmitted in a multi-node communication network  Bart E. Rice
5452328 (08/100334)	US	9/19/1995 (7/30/1993)	Technique for generating sets of binary spreading-code sequences for a high data-rate spread-spectrum network  Bart F. Rice
5815526 (08/456077)	US	9/29/1998 (5/31/1995)	Signal comprising binary spreading-code sequences  Bart F. Rice

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
5991333 (09/113410)	US	11/23/1999 (7/10/1998)	Spread-spectrum transceiver Bart F. Rice
7760792 (09/759425)	US	7/20/2010 (1/12/2001)	Spread spectrum electromagnetic signals Bart F. Rice
7457345 (10/873784)	US	11/25/2008 (6/21/2004)	Spread-spectrum transceiver Bart E. Rice
7457348 (11/468923)	US	11/25/2008 (8/31/2006)	Spread-spectrum transceiver Bart F. Rice
7924906 (11/470967)	US	4/12/2011 (9/7/2006)	SPREAD-SPECTRUM RECEIVER Bart F. Rice
(12/755012)	US	(4/6/2010)	SPREAD SPECTRUM TRANSCEIVER Bart F. Rice
7706247 (11/504249)	US	4/27/2010 (8/14/2006)	Frequency offset differential pulse position modulation Michael Mancusi
(09/584057)	US	(5/30/2000)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT Seth Elliott
(11/423847)	US	(6/13/2006)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT Seth Elliott
6710424 (09/962717)	US	3/23/2004 (9/21/2001)	RF CHIPSET ARCHITECTURE Dominik J. Schmidt

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
6667967 (09/500887)	US	12/23/2003 (2/9/2000)	HIGH-SPEED NETWORK OF INDEPENDENTLY LINKED NODES  Richard H. Christensen
(11/147853)	US	(6/8/2005)	SYSTEM AND METHOD FOR DISTRIBUTING ADDRESSES  Keith R. Anderson
(11/514294)	US	(8/31/2006)	NEIGHBORHOOD AREA NETWORK WITH RING BACKBONE TOPOLOGY  Keith R. Anderson
FR2794311 (FR9906710)	FR	12/14/2007 (5/27/1999)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION  MORCHE, Dominique
GB1183777 (GB00936952.1)	GB	7/30/2003 (5/26/2000)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION  MORCHE, Dominique
IT1183777 (IT00936952.1)	IT	7/30/2003 (5/26/2000)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION  MORCHE, Dominique
7555273 (11/330275)	US	6/30/2009 (1/11/2006)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION  MORCHE, Dominique
(PCT/US2001/015840)	WO	(5/16/2001)	DOUBLE POWER-EYE SAFE LASER OUTPUT  ALWAN JAMES J

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(10/287109)	US	(11/1/2002)	MULTI-CHANNEL OPTICAL TRANSCIVER  Scott H. Bloom
(PCT/US2001/030144)	WO	(9/27/2001)	SYSTEMS & METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
(11/447279)	US	(6/6/2006)	SYSTEMS AND METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
(11/256618)	US	(10/21/2005)	TRACKING OF MOBILE TERMINAL EQUIPMENT IN A MOBILE COMMUNICATIONS SYSTEM  TORKKI, Markus
(PCT/US2002/012963)	WO	(4/26/2002)	AUDIO CALLING NAME SERVICE  WORSHAM JAMES A
(11/724311)	US	(3/15/2007)	AUDIO CALLING NAME AND NUMBER DELIVERY  WORSHAM JAMES A
6873686 (09/634793)	US	3/29/2005 (8/9/2000)	NETWORK AND METHOD FOR PROVIDING A CALLING NAME TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(60/213827)	US	(6/23/2000)	Method of cross-promoting and monetizing web sites by means of audio advertisement  Brian Mark Shuster
(60/213396)	US	(6/23/2000)	Method of delivering audio commerical advertisements  Brian Mark Schuster
(60/226108)	US	(8/17/2000)	Method and system of increasing user response to audio advertisements on the internet  Brian Mark Shuster
(60/225943)	US	(8/17/2000)	Method and system of enhancing the effectiveness of audio advertisements on the internet  Brian Mark Shuster
(09/893362)	US	(6/25/2001)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK  Brian Mark Shuster
(13/353787)	US	(1/19/2012)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK  Brian Mark Shuster
(60/225888)	US	(8/17/2000)	Application and method for maximizing the value of bandwidth usage on wide area networks  Gary Stephen Shuster
(60/190646)	US	(3/20/2000)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC)

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Steven W. Smith
(09/686598)	US	(10/10/2000)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC)  Steven W. Smith
(PCT/US2002/015636)	WO	(5/17/2002)	Method and system for remote utilizing a mobile device to share data objects  Richard A Pineau
(EP02774105.7)	EP	(5/17/2002)	Method and system for remote utilizing a mobile device to share data objects  Richard A Pineau
(JP2003-500782)	JP	(5/17/2002)	METHOD AND SYSTEM FOR REMOTE UTILIZING A MOBILE DEVICE TO SHARE DATA OBJECTS  Richard A Pineau
(11/725192)	US	(3/15/2007)	WIDE AREA REAL-TIME SOFTWARE ENVIRONMENT  Greg Lane
(PCT/US2001/004776)	WO	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY
(CA2400388)	CA	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY
(EP01909237.8)	EP	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY



<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
6985561 (10/853642)	US	1/10/2006 (5/26/2004)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Raymond J. Smets
(PCT/US2002/040139)	WO	(12/13/2002)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  CHANG E-LEE
(12/046610)	US	(3/12/2008)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  Linda Ann Roberts
(60/196095)	US	(4/11/2000)	Prepaid/postpaid automatic change of payment option  Dara Ung
FI4119 (FI990238)	FI	8/31/1999 (2/8/1999)	Optical add/drop multiplexer  Ari Tervonen
(PCT/FI2000/000082)	WO	(2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER  Ari Tervonen
EP1151567 (EP00903718.5)	EP	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER  Ari Tervonen
7769374 (09/802861)	US	8/3/2010 (3/12/2001)	RECOVERY TECHNIQUES IN MOBILE NETWORKS  Heikki Juhani Einola
(15/887481)	US	(2/2/2018)	RECOVERY TECHNIQUES IN MOBILE NETWORKS  Heikki Juhani Einola

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(10/063268)	US	(4/4/2002)	System and method for implementing dynamic scheduling of data in a non-blocking all-optical switching network  Robert E. Best
(60/246821)	US	(11/7/2000)	Method and system for passing business objects  Marc Asheghian
(10/012240)	US	(11/5/2001)	Method and system for passing business objects  Philippe Richard
(60/403873)	US	(8/16/2002)	MANAGED INFORMATION TRANSMISSION IN A NETWORK ENVIRONMENT  Phillippe Richard
(60/484885)	US	(7/3/2003)	MANAGED INFORMATION TRANSMISSION OF ELECTRONIC MAIL IN A NETWORK ENVIRONMENT  Phillippe Richard
(10/643734)	US	(8/18/2003)	Managed information transmission of electronic items in a network environment  Phillippe Richard
(60/590489)	US	(7/22/2004)	Adaptive data transformation engine  Phillippe Richard
(PCT/US2001/032613)	WO	(10/18/2001)	DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS  CRAWFORD JAMES A

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/US2001/044619)	WO	(11/27/2001)	CARD-BASED DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS  James A. Crawford
(PCT/US2001/047183)	WO	(10/30/2001)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS  CRAWFORD JAMES A
TWI171699 (TW090127391)	TW	1/11/2003 (11/5/2001)	Transmission security for wireless communications  CRAWFORD JAMES A
6650616 (10/178207)	US	11/18/2003 (6/24/2002)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS  James A. Crawford

Assignor assigns to Assignee all of its rights to the inventions, invention disclosures, and discoveries in the assets listed above, together, with its rights, if any, to revive prosecution of claims under such assets and to sue or otherwise enforce any claims under such assets for past, present or future infringement.

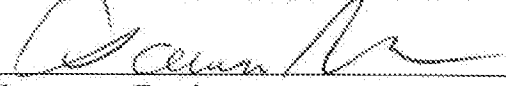
Assignor hereby authorizes the respective patent office or governmental agency in each jurisdiction to make available to Assignee all records regarding the Certain Assets.

The terms and conditions of this Assignment of Rights in Certain Assets will inure to the benefit of Assignee, its successors, assigns, and other legal representatives and will be binding upon Assignor, its successors, assigns, and other legal representatives.

EXECUTED this 15<sup>th</sup> day of November, 2019, to be effective as of  
November 15, 2019.

ASSIGNOR:

INTELLECTUAL VENTURES ASSETS 135 LLC

By:   
Name: Lawrence Froeber  
Title: CFO

# Exhibit X

---

**PATENT ASSIGNMENT COVER SHEET**Electronic Version v1.1  
Stylesheet Version v1.2

EPAS ID: PAT5892339

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT	
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT	
<b>CONVEYING PARTY DATA</b>		
<b>Name</b>		<b>Execution Date</b>
INTELLECTUAL VENTURES ASSETS 130 LLC		11/15/2019
<b>RECEIVING PARTY DATA</b>		
<b>Name:</b>	COMMWORKS SOLUTIONS, LLC	
<b>Street Address:</b>	44 MILTON AVENUE	
<b>Internal Address:</b>	SUITE 254	
<b>City:</b>	ALPHARETTA	
<b>State/Country:</b>	GEORGIA	
<b>Postal Code:</b>	30009	
<b>PROPERTY NUMBERS Total: 35</b>		
<b>Property Type</b>	<b>Number</b>	
Patent Number:	7050962	
Patent Number:	7266490	
Patent Number:	7289456	
Patent Number:	6975622	
Patent Number:	7477703	
Patent Number:	6975855	
Patent Number:	6341221	
Patent Number:	7555014	
Application Number:	60193169	
Application Number:	10158772	
Application Number:	11557057	
Application Number:	11557053	
Application Number:	13766960	
Application Number:	60380425	
Application Number:	10437129	
Application Number:	60557954	
Application Number:	10816481	
Application Number:	11076738	
Application Number:	11095349	

**PATENT**

505845403

**REEL: 051407 FRAME: 0106**

Property Type	Number
Application Number:	60747409
Application Number:	15935928
Application Number:	60614609
Application Number:	60121552
Application Number:	60139471
Application Number:	60485880
Application Number:	60229317
Application Number:	10681562
Application Number:	10542183
Application Number:	60299454
Application Number:	60193402
Application Number:	10225457
Application Number:	10378068
Application Number:	60225603
Application Number:	11741894
Application Number:	60224031

**CORRESPONDENCE DATA**

**Fax Number:** (404)645-7707

*Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.*

**Phone:** 4046457700

**Email:** docketing@mcciplaw.com

**Correspondent Name:** LAWRENCE AARONSON

**Address Line 1:** 999 PEACHTREE STREET NE

**Address Line 2:** SUITE 1300

**Address Line 4:** ATLANTA, GEORGIA 30309

**ATTORNEY DOCKET NUMBER:** 11201-001GEN

**NAME OF SUBMITTER:** LAWRENCE A. AARONSON

**SIGNATURE:** /Lawrence A. Aaronson/

**DATE SIGNED:** 01/03/2020

**Total Attachments: 14**

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page1.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page2.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page3.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page4.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page5.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page6.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page7.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page8.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page9.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page10.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page11.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page12.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page13.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page14.tif



**Exhibit B-2****ASSIGNMENT OF RIGHTS IN CERTAIN ASSETS**

For good and valuable consideration, the receipt of which is hereby acknowledged, Intellectual Ventures Assets 130 LLC, a Delaware limited liability company, with an address at 251 Little Falls Drive, Wilmington, DE 19808 ("**Assignor**"), does hereby sell, assign, transfer, and convey unto CommWorks Solutions, LLC, a Georgia limited liability company with an address at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009 ("**Assignee**"), its right, title, and interest in and to any and all of the following provisional patent applications, patent applications, patents, and other governmental grants or issuances of any kind (the "**Certain Assets**");

**Inactive Patent(s) – (Abandoned; Lapsed; Expired)**

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
EP1150530 (EP01102111.0)	EP	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
SE1150530 (SE01102111.0)	SE	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
(60/193169)	US	(3/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7050962 (09/751573)	US	5/23/2006 (12/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7266490 (10/158648)	US	9/4/2007 (5/31/2002)	Apparatus and method for connecting hardware to a circuit simulation  Robert Marc Zeidman
(10/158772)	US	(5/31/2002)	Apparatus and method for connecting a hardware emulator to a computer peripheral  Robert Marc Zeidman
(11/557057)	US	(11/6/2006)	APPARATUS AND METHOD FOR CONNECTING A HARDWARE EMULATOR TO A COMPUTER PERIPHERAL

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Robert Marc Zeidman
(11/557053)	US	(11/6/2006)	SYSTEM AND METHOD FOR CONNECTING A LOGIC CIRCUIT SIMULATION TO A NETWORK  Robert M. Ziedman
(13/766960)	US	(2/14/2013)	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
(60/380425)	US	(5/13/2002)	Low cost, minimal software footprint, self configuring, ad hoc, autonomic networking apparatus and method of use  Michael P. Nova
(10/437129)	US	(5/13/2003)	SYSTEMS AND METHODS FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  Michael P. Nova
(PCT/US2003/034799)	WO	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W
(CN200380110363.0)	CN	(10/31/2003)	System and method for routing packets in a wired or wireless network  GILLIES DONALD W WANG WEILIN N
(EP03778062.4)	EP	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/US2003/034884)	WO	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF A WIRED OR WIRELESS NETWORK  NOVA MICHAEL P
(CN200380110362.6)	CN	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  GILLIES DONALD W WANG WEILIN N
(EP03778075.6)	EP	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  WANG WEILIN
(60/557954)	US	(3/31/2004)	Broadband applications for wireless mesh networks  Weilin Wang
(10/816481)	US	(4/1/2004)	Systems and methods for congestion control in a wireless mesh network  Michael P. Nova
(11/076738)	US	(3/9/2005)	Distributed TDMA for wireless mesh network  Weilin Wang
(11/095349)	US	(3/31/2005)	SYSTEMS AND METHODS FOR BROADBAND DATA COMMUNICATION IN A WIRELESS MESH NETWORK  Weilin Wang
(60/747409)	US	(5/16/2006)	Distributed Multi-Channel TDMA MAC for Wireless Mesh Networks  Xudong Wang

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/US2007/069031)	WO	(5/16/2007)	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION  GUI CHAO
(PCT/US2007/070225)	WO	(6/1/2007)	SYSTEM AND METHOD FOR TRANSPARENT WIRELESS BRIDGING OF COMMUNICATION CHANNEL SEGMENTS  RIMMER JAMES
(15/935928)	US	(3/26/2018)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Weilin Wang
7289456 (10/118187)	US	10/30/2007 (4/8/2002)	Determining and provisioning paths within a network of communication elements  Gupta, Sanyogita
(60/614609)	US	(9/30/2004)	Modeling of topology connectivity map for efficient layer 1 routing  Sanyogita Gupta
(PCT/US2005/034418)	WO	(9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
EP1797670 (EP05857725.5)	EP	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
(60/121552)	US	(2/25/1999)	Adaptive mobility-aware signaling for wireless IP telephony  Agrawal, Prathima
(PCT/US2000/004629)	WO	(2/24/2000)	Adaptive signaling and mobility for wireless telephony

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Agrawal, Prathima
(60/139471)	US	(6/16/1999)	PCS-to-mobile IP internetworking Chang, Li-Fung
(PCT/US2000/014059)	WO	(5/22/2000)	ACTIVE LINK LAYER AND INTRA-DOMAIN MOBILITY FOR IP NETWORKS AGRAWAL PRATHIMA
(60/485880)	US	(7/8/2003)	Enhanced Phone-Based Collaboration Korycki, Jacek
6975622 (10/756526)	US	12/13/2005 (1/13/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
(PCT/US2004/021407)	WO	(7/2/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
SE522377 (SE0001148-6)	SE	2/3/2004 (3/31/2000)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
(PCT/SE2001/000423)	WO	(2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
EP1269688 (EP01910283.9)	EP	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
DE60145827.3 (DE60145827.3)	DE	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
FR1269688 (FR01910283.9)	FR	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
GB1269688 (GB01910283.9)	GB	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
(60/229317)	US	(8/30/2000)	Personal digital assistant based communication system  Bloomfield, Mark C.
(PCT/US2001/023402)	WO	(7/26/2001)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(10/681562)	US	(10/8/2003)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(PCT/US1997/018071)	WO	(10/7/1997)	Unable to verify  Unable to Verify
(PCT/US2004/000860)	WO	(1/13/2004)	Time based wireless access provisioning  Roskind, James A.

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(10/542183)	US	(7/13/2005)	Time based wireless access provisioning Roskind, James
(60/299454)	US	(6/21/2001)	Client device identification when communicating through a network address translator device Rodriguez-Val, Richard
(EP01912047.6)	EP	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system Van Valkenburg, Sander
(PCT/IB2001/000352)	WO	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system Van Valkenburg, Sander
FI112565 (FI20000406)	FI	2003-12-15_Salesforce (2/22/2000)	METHOD AND RADIO SYSTEM FOR DIGITAL SIGNAL TRANSMISSION HOTTINEN,ARI
(60/193402)	US	(3/29/2000)	Class of space-time block codes for more than two transmit antennas Boariu, Adrian
(FI20001944)	FI	(9/4/2000)	Method and arrangement for digital signal transmission Tirkkonen, Olav
(PCT/FI2000/000916)	WO	(10/23/2000)	Method and arrangement for digital signal transmission Tirkkonen, Olav
EP1336268 (EP00969617.0)	EP	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission



<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Tirkkonen, Olav
DE60048671.0 (DE60048671.0)	DE	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
FR11336268 (FR00969617.0)	FR	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
GB1336268 (GB00969617.0)	GB	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
(FI20002845)	FI	(12/22/2000)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2001/000166)	WO	(2/20/2001)	Method and radio system for digital signal transmission  Tirkkonen, Olav
(EP01911785.2)	EP	(2/20/2001)	Method and radio system for digital signal transmission  Tirkkonen, Olav
(FI20011357)	FI	(6/25/2001)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2001/001133)	WO	(12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
EP1350354 (EP01273305.1)	EP	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2002/000553)	WO	(6/24/2002)	Transmission method  Tirkkonen, Olav

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
EP1405453 (EP02743313.5)	EP	1/2/2013 (6/24/2002)	Transmission method Tirkkonen, Olav
(10/225457)	US	(8/22/2002)	Method and radio system for digital signal transmission Ari Hottinen
(10/378068)	US	(3/4/2003)	Method and arrangement for digital signal transmission Tirkkonen, Olav
7477703 (11/070717)	US	1/13/2009 (3/2/2005)	Method and radio system for digital signal transmission using complex space-time codes Tirkkonen, Olav
(MX03009987)	MX	(10/31/2003)	RFID system and method for ensuring safety of hazardous or dangerous substances Reade, Walter Caswell
FI106507 (FI980824)	FI	2/15/2001 (4/9/1998)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
(PCT/FI1999/000300)	WO	(4/9/1999)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
FI108604 (FI990963)	FI	2/15/2002 (4/28/1999)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka
(PCT/FI2000/000359)	WO	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(EP00920786.1)	EP	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES  Wallenius, Jukka
6975855 (09/958065)	US	12/13/2005 (4/26/2000)	Method for managing mobile station facilities  Wallenius, Jukka
FI108979 (FI991360)	FI	4/30/2002 (6/14/1999)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
(PCT/FI2000/000530)	WO	(6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
EP1192811 (EP00942154.6)	EP	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
FR1192811 (FR00942154.6)	FR	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
(JP2001-504184)	JP	(6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
FI109506 (FI981113)	FI	8/15/2002 (5/9/1998)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/FI1999/000430)	WO	(5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
CNZL99806247.2 (CN99806247.2)	CN	2/18/2004 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
EP1080587 (EP99952144.6)	EP	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  HUOTARI SEPPU
DE69934114.0 (DE69934114.0)	DE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
ES1080587 (ES99952144.6)	ES	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
FR1080587 (FR99952144.6)	FR	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
GB1080587 (GB99952144.6)	GB	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Huotari, Seppo
IT1080587 (IT99952144.6)	IT	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
NL1080587 (NL99952144.6)	NL	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
SE1080587 (SE99952144.6)	SE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
6341221 (09/702495)	US	1/22/2002 (10/31/2000)	Method of managing a subscriber service by an intelligent network service  Huotari, Seppo
(PCT/EP1999/010097)	WO	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
(EP99965493.2)	EP	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
7555014 (11/402621)	US	6/30/2009 (4/11/2006)	METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
(60/225603)	US	(8/15/2000)	Cellular network independent short message delivery system

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Simon Bennett
(PCT/US2001/024475)	WO	(8/2/2001)	Method And Apparatus For A Network Independent Short Message Delivery System  Simon Bennett
(11/741894)	US	(4/30/2007)	Wireless sensor data processing systems  Bao Q. Tran
(60/224031)	US	(8/9/2000)	Non-intrusive coupler for a broadband communications system using high voltage shielded power distributed cables  Paul A. Kline
(PCT/US2005/041148)	WO	(11/14/2005)	Power line coupling device and method of using the same  William O. Radtke
(EP05849637.3)	EP	(11/14/2005)	Power line coupling device and method of using the same  William O. Radtke
(PCT/US2001/011311)	WO	(4/6/2001)	Method and system for scheduling inbound inquiries  Daniel N. Duncan
JP3810956  (JP11-212974)	JP	6/2/2006  (7/28/1999)	Operational supervisory system for a server  Miwa Nishio

Assignor assigns to Assignee all of its rights to the inventions, invention disclosures, and discoveries in the assets listed above, together, with its rights, if any, to revive prosecution of claims under such assets and to sue or otherwise enforce any claims under such assets for past, present or future infringement.

Assignor hereby authorizes the respective patent office or governmental agency in each jurisdiction to make available to Assignee all records regarding the Certain Assets.

The terms and conditions of this Assignment of Rights in Certain Assets will inure to the benefit of Assignee, its successors, assigns, and other legal representatives and will be binding upon Assignor, its successors, assigns, and other legal representatives.

EXECUTED this 15<sup>th</sup> day of November, 2019, to be effective as of  
November 15, 2019.

ASSIGNOR:

INTELLECTUAL VENTURES ASSETS 130 LLC

By: 

Name: Lawrence Froeber

Title: CFO



# Exhibit Y

---

## PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1  
 Stylesheet Version v1.2

EPAS ID: PAT5892339

<b>SUBMISSION TYPE:</b>	NEW ASSIGNMENT	
<b>NATURE OF CONVEYANCE:</b>	ASSIGNMENT	
<b>CONVEYING PARTY DATA</b>		
<b>Name</b>		<b>Execution Date</b>
INTELLECTUAL VENTURES ASSETS 130 LLC		11/15/2019
<b>RECEIVING PARTY DATA</b>		
<b>Name:</b>	COMMWORKS SOLUTIONS, LLC	
<b>Street Address:</b>	44 MILTON AVENUE	
<b>Internal Address:</b>	SUITE 254	
<b>City:</b>	ALPHARETTA	
<b>State/Country:</b>	GEORGIA	
<b>Postal Code:</b>	30009	
<b>PROPERTY NUMBERS Total: 35</b>		
<b>Property Type</b>	<b>Number</b>	
Patent Number:	7050962	
Patent Number:	7266490	
Patent Number:	7289456	
Patent Number:	6975622	
Patent Number:	7477703	
Patent Number:	6975855	
Patent Number:	6341221	
Patent Number:	7555014	
Application Number:	60193169	
Application Number:	10158772	
Application Number:	11557057	
Application Number:	11557053	
Application Number:	13766960	
Application Number:	60380425	
Application Number:	10437129	
Application Number:	60557954	
Application Number:	10816481	
Application Number:	11076738	
Application Number:	11095349	

PATENT

505845403

REEL: 051407 FRAME: 0106

Property Type	Number
Application Number:	60747409
Application Number:	15935928
Application Number:	60614609
Application Number:	60121552
Application Number:	60139471
Application Number:	60485880
Application Number:	60229317
Application Number:	10681562
Application Number:	10542183
Application Number:	60299454
Application Number:	60193402
Application Number:	10225457
Application Number:	10378068
Application Number:	60225603
Application Number:	11741894
Application Number:	60224031

**CORRESPONDENCE DATA**

**Fax Number:** (404)645-7707

*Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.*

**Phone:** 4046457700

**Email:** docketing@mcciplaw.com

**Correspondent Name:** LAWRENCE AARONSON

**Address Line 1:** 999 PEACHTREE STREET NE

**Address Line 2:** SUITE 1300

**Address Line 4:** ATLANTA, GEORGIA 30309

<b>ATTORNEY DOCKET NUMBER:</b>	11201-001GEN
<b>NAME OF SUBMITTER:</b>	LAWRENCE A. AARONSON
<b>SIGNATURE:</b>	/Lawrence A. Aaronson/
<b>DATE SIGNED:</b>	01/03/2020

**Total Attachments: 14**

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page1.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page2.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page3.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page4.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page5.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page6.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page7.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page8.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page9.tif

source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page10.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page11.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page12.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page13.tif  
source=IV 130 to CommWorks Solutions (Lapsed-Expired)#page14.tif

**Exhibit B-2****ASSIGNMENT OF RIGHTS IN CERTAIN ASSETS**

For good and valuable consideration, the receipt of which is hereby acknowledged, Intellectual Ventures Assets 130 LLC, a Delaware limited liability company, with an address at 251 Little Falls Drive, Wilmington, DE 19808 ("**Assignor**"), does hereby sell, assign, transfer, and convey unto CommWorks Solutions, LLC, a Georgia limited liability company with an address at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009 ("**Assignee**"), its right, title, and interest in and to any and all of the following provisional patent applications, patent applications, patents, and other governmental grants or issuances of any kind (the "**Certain Assets**");

**Inactive Patent(s) – (Abandoned; Lapsed; Expired)**

<b><u>Patent/Application Number</u></b>	<b><u>Country</u></b>	<b><u>Issue Date/ Filing Date</u></b>	<b><u>Title of Patent and First Named Inventor</u></b>
EP1150530 (EP01102111.0)	EP	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
SE1150530 (SE01102111.0)	SE	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
(60/193169)	US	(3/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7050962 (09/751573)	US	5/23/2006 (12/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7266490 (10/158648)	US	9/4/2007 (5/31/2002)	Apparatus and method for connecting hardware to a circuit simulation  Robert Marc Zeidman
(10/158772)	US	(5/31/2002)	Apparatus and method for connecting a hardware emulator to a computer peripheral  Robert Marc Zeidman
(11/557057)	US	(11/6/2006)	APPARATUS AND METHOD FOR CONNECTING A HARDWARE EMULATOR TO A COMPUTER PERIPHERAL

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Robert Marc Zeidman
(11/557053)	US	(11/6/2006)	SYSTEM AND METHOD FOR CONNECTING A LOGIC CIRCUIT SIMULATION TO A NETWORK  Robert M. Ziedman
(13/766960)	US	(2/14/2013)	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
(60/380425)	US	(5/13/2002)	Low cost, minimal software footprint, self configuring, ad hoc, autonomic networking apparatus and method of use  Michael P. Nova
(10/437129)	US	(5/13/2003)	SYSTEMS AND METHODS FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  Michael P. Nova
(PCT/US2003/034799)	WO	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W
(CN200380110363.0)	CN	(10/31/2003)	System and method for routing packets in a wired or wireless network  GILLIES DONALD W WANG WEILIN N
(EP03778062.4)	EP	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/US2003/034884)	WO	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF A WIRED OR WIRELESS NETWORK  NOVA MICHAEL P
(CN200380110362.6)	CN	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  GILLIES DONALD W WANG WEILIN N
(EP03778075.6)	EP	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  WANG WEILIN
(60/557954)	US	(3/31/2004)	Broadband applications for wireless mesh networks  Weilin Wang
(10/816481)	US	(4/1/2004)	Systems and methods for congestion control in a wireless mesh network  Michael P. Nova
(11/076738)	US	(3/9/2005)	Distributed TDMA for wireless mesh network  Weilin Wang
(11/095349)	US	(3/31/2005)	SYSTEMS AND METHODS FOR BROADBAND DATA COMMUNICATION IN A WIRELESS MESH NETWORK  Weilin Wang
(60/747409)	US	(5/16/2006)	Distributed Multi-Channel TDMA MAC for Wireless Mesh Networks  Xudong Wang



<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/US2007/069031)	WO	(5/16/2007)	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION  GUI CHAO
(PCT/US2007/070225)	WO	(6/1/2007)	SYSTEM AND METHOD FOR TRANSPARENT WIRELESS BRIDGING OF COMMUNICATION CHANNEL SEGMENTS  RIMMER JAMES
(15/935928)	US	(3/26/2018)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Weilin Wang
7289456 (10/118187)	US	10/30/2007 (4/8/2002)	Determining and provisioning paths within a network of communication elements  Gupta, Sanyogita
(60/614609)	US	(9/30/2004)	Modeling of topology connectivity map for efficient layer 1 routing  Sanyogita Gupta
(PCT/US2005/034418)	WO	(9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
EP1797670 (EP05857725.5)	EP	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
(60/121552)	US	(2/25/1999)	Adaptive mobility-aware signaling for wireless IP telephony  Agrawal, Prathima
(PCT/US2000/004629)	WO	(2/24/2000)	Adaptive signaling and mobility for wireless telephony

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Agrawal, Prathima
(60/139471)	US	(6/16/1999)	PCS-to-mobile IP internetworking Chang, Li-Fung
(PCT/US2000/014059)	WO	(5/22/2000)	ACTIVE LINK LAYER AND INTRA-DOMAIN MOBILITY FOR IP NETWORKS AGRAWAL PRATHIMA
(60/485880)	US	(7/8/2003)	Enhanced Phone-Based Collaboration Korycki, Jacek
6975622 (10/756526)	US	12/13/2005 (1/13/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
(PCT/US2004/021407)	WO	(7/2/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
SE522377 (SE0001148-6)	SE	2/3/2004 (3/31/2000)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
(PCT/SE2001/000423)	WO	(2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
EP1269688 (EP01910283.9)	EP	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
DE60145827.3 (DE60145827.3)	DE	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
FR1269688 (FR01910283.9)	FR	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
GB1269688 (GB01910283.9)	GB	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
(60/229317)	US	(8/30/2000)	Personal digital assistant based communication system  Bloomfield, Mark C.
(PCT/US2001/023402)	WO	(7/26/2001)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(10/681562)	US	(10/8/2003)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(PCT/US1997/018071)	WO	(10/7/1997)	Unable to verify  Unable to Verify
(PCT/US2004/000860)	WO	(1/13/2004)	Time based wireless access provisioning  Roskind, James A.

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(10/542183)	US	(7/13/2005)	Time based wireless access provisioning Roskind, James
(60/299454)	US	(6/21/2001)	Client device identification when communicating through a network address translator device Rodriguez-Val, Richard
(EP01912047.6)	EP	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system Van Valkenburg, Sander
(PCT/IB2001/000352)	WO	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system Van Valkenburg, Sander
FI112565 (FI20000406)	FI	2003-12-15_Salesforce (2/22/2000)	METHOD AND RADIO SYSTEM FOR DIGITAL SIGNAL TRANSMISSION HOTTINEN,ARI
(60/193402)	US	(3/29/2000)	Class of space-time block codes for more than two transmit antennas Boariu, Adrian
(FI20001944)	FI	(9/4/2000)	Method and arrangement for digital signal transmission Tirkkonen, Olav
(PCT/FI2000/000916)	WO	(10/23/2000)	Method and arrangement for digital signal transmission Tirkkonen, Olav
EP1336268 (EP00969617.0)	EP	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Tirkkonen, Olav
DE60048671.0 (DE60048671.0)	DE	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
FR11336268 (FR00969617.0)	FR	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
GB1336268 (GB00969617.0)	GB	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
(FI20002845)	FI	(12/22/2000)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2001/000166)	WO	(2/20/2001)	Method and radio system for digital signal transmission  Tirkkonen, Olav
(EP01911785.2)	EP	(2/20/2001)	Method and radio system for digital signal transmission  Tirkkonen, Olav
(FI20011357)	FI	(6/25/2001)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2001/001133)	WO	(12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
EP1350354 (EP01273305.1)	EP	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
(PCT/FI2002/000553)	WO	(6/24/2002)	Transmission method  Tirkkonen, Olav

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
EP1405453 (EP02743313.5)	EP	1/2/2013 (6/24/2002)	Transmission method Tirkkonen, Olav
(10/225457)	US	(8/22/2002)	Method and radio system for digital signal transmission Ari Hottinen
(10/378068)	US	(3/4/2003)	Method and arrangement for digital signal transmission Tirkkonen, Olav
7477703 (11/070717)	US	1/13/2009 (3/2/2005)	Method and radio system for digital signal transmission using complex space-time codes Tirkkonen, Olav
(MX03009987)	MX	(10/31/2003)	RFID system and method for ensuring safety of hazardous or dangerous substances Reade, Walter Caswell
FI106507 (FI980824)	FI	2/15/2001 (4/9/1998)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
(PCT/FI1999/000300)	WO	(4/9/1999)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
FI108604 (FI990963)	FI	2/15/2002 (4/28/1999)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka
(PCT/FI2000/000359)	WO	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(EP00920786.1)	EP	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES  Wallenius, Jukka
6975855 (09/958065)	US	12/13/2005 (4/26/2000)	Method for managing mobile station facilities  Wallenius, Jukka
FI108979 (FI991360)	FI	4/30/2002 (6/14/1999)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
(PCT/FI2000/000530)	WO	(6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
EP1192811 (EP00942154.6)	EP	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
FR1192811 (FR00942154.6)	FR	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
(JP2001-504184)	JP	(6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
FI109506 (FI981113)	FI	8/15/2002 (5/9/1998)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo



<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
(PCT/FI1999/000430)	WO	(5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
CNZL99806247.2 (CN99806247.2)	CN	2/18/2004 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
EP1080587 (EP99952144.6)	EP	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  HUOTARI SEPPO
DE69934114.0 (DE69934114.0)	DE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
ES1080587 (ES99952144.6)	ES	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
FR1080587 (FR99952144.6)	FR	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
GB1080587 (GB99952144.6)	GB	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Huotari, Seppo
IT1080587 (IT99952144.6)	IT	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
NL1080587 (NL99952144.6)	NL	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
SE1080587 (SE99952144.6)	SE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
6341221 (09/702495)	US	1/22/2002 (10/31/2000)	Method of managing a subscriber service by an intelligent network service  Huotari, Seppo
(PCT/EP1999/010097)	WO	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
(EP99965493.2)	EP	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
7555014 (11/402621)	US	6/30/2009 (4/11/2006)	METHOD FOR CONTENTION FREE TRAFFIC DETECTION  Hautala Petri
(60/225603)	US	(8/15/2000)	Cellular network independent short message delivery system

<u>Patent/Application Number</u>	<u>Country</u>	<u>Issue Date/ Filing Date</u>	<u>Title of Patent and First Named Inventor</u>
			Simon Bennett
(PCT/US2001/024475)	WO	(8/2/2001)	Method And Apparatus For A Network Independent Short Message Delivery System  Simon Bennett
(11/741894)	US	(4/30/2007)	Wireless sensor data processing systems  Bao Q. Tran
(60/224031)	US	(8/9/2000)	Non-intrusive coupler for a broadband communications system using high voltage shielded power distributed cables  Paul A. Kline
(PCT/US2005/041148)	WO	(11/14/2005)	Power line coupling device and method of using the same  William O. Radtke
(EP05849637.3)	EP	(11/14/2005)	Power line coupling device and method of using the same  William O. Radtke
(PCT/US2001/011311)	WO	(4/6/2001)	Method and system for scheduling inbound inquiries  Daniel N. Duncan
JP3810956  (JP11-212974)	JP	6/2/2006  (7/28/1999)	Operational supervisory system for a server  Miwa Nishio

Assignor assigns to Assignee all of its rights to the inventions, invention disclosures, and discoveries in the assets listed above, together, with its rights, if any, to revive prosecution of claims under such assets and to sue or otherwise enforce any claims under such assets for past, present or future infringement.

Assignor hereby authorizes the respective patent office or governmental agency in each jurisdiction to make available to Assignee all records regarding the Certain Assets.

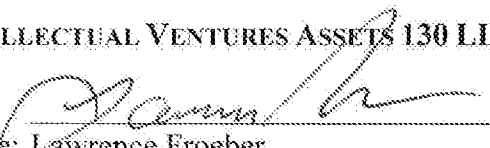
The terms and conditions of this Assignment of Rights in Certain Assets will inure to the benefit of Assignee, its successors, assigns, and other legal representatives and will be binding upon Assignor, its successors, assigns, and other legal representatives.

EXECUTED this 15<sup>th</sup> day of November, 2019, to be effective as of  
November 15, 2019.

ASSIGNOR:

INTELLECTUAL VENTURES ASSETS 130 LLC

By:

  
Name: Lawrence Froeber

Title: CFO

# Exhibit Z

---

**UCC FINANCING STATEMENT**

FOLLOW INSTRUCTIONS

<b>A. NAME &amp; PHONE OF CONTACT AT FILER (optional)</b> UNISEARCH, INC. 360-956-9500
<b>B. E-MAIL CONTACT AT FILER (optional)</b> Kristy.Bertsch@unisearch.com
<b>C. SEND ACKNOWLEDGMENT TO: (Name and Address)</b>  UNISEARCH 1780 BARNES BLVD SW TUMWATER, WA 98512

CTY# YEAR UCC #  
0602019-09450  
Filed and Recorded Dec-05-2019 03:39pm  
CATHELENE ROBINSON  
Clerk of Superior Court  
Fulton County, Georgia

THE ABOVE SPACE IS FOR FILING OFFICE USE ONLY

1. DEBTOR'S NAME: Provide only one Debtor name (1a or 1b) (use exact, full name; do not omit, modify, or abbreviate any part of the Debtor's name); if any part of the individual Debtor's name will not fit in line 1b, leave all of Item 1 blank, check here ☐ and provide the individual Debtor information in Item 10 of the Financing Statement Addendum (Form UCC1Ad)

1a. ORGANIZATION'S NAME CommWorks Solutions, LLC				
OR	1b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
1c. MAILING ADDRESS 44 Milton Avenue, Suite 254		CITY Alpharetta	STATE GA	POSTAL CODE 30009
			COUNTRY USA	

2. DEBTOR'S NAME: Provide only one Debtor name (2a or 2b) (use exact, full name; do not omit, modify, or abbreviate any part of the Debtor's name); if any part of the individual Debtor's name will not fit in line 2b, leave all of Item 2 blank, check here ☐ and provide the individual Debtor information in Item 10 of the Financing Statement Addendum (Form UCC1Ad)

2a. ORGANIZATION'S NAME				
OR	2b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
2c. MAILING ADDRESS		CITY	STATE	POSTAL CODE
			COUNTRY USA	

3. SECURED PARTY'S NAME (or NAME of ASSIGNEE of ASSIGNOR SECURED PARTY): Provide only one Secured Party name (3a or 3b)

3a. ORGANIZATION'S NAME Intellectual Ventures Assets 135 LLC				
OR	3b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
3c. MAILING ADDRESS 251 Little Falls Drive		CITY Wilmington	STATE DE	POSTAL CODE 19808
			COUNTRY USA	

4. COLLATERAL: This financing statement covers the following collateral:

A first priority security interest in all Collateral to secure all present and future payment and performance obligations of Debtor to Secured Party or any of Secured Party's affiliates, including, without limitation, Debtor's obligations under the PSA (collectively, the "Obligations"). "Collateral" means the Assigned Patent Rights and the Certain Other Assets, and all Revenue (as such term is defined in the PSA).

It is understood and agreed that any Revenue that is properly distributed to either Secured Party or any of Secured Party's Affiliates or Debtor and/or its Affiliates in accordance with the terms and conditions of the PSA are not considered Collateral under this Security Interest Addendum.

Additional Collateral included on Attachment A.

5. Check only if applicable and check only one box: Collateral is <input type="checkbox"/> held in a Trust (see UCC1Ad, Item 17 and instructions) <input type="checkbox"/> being administered by a Decedent's Personal Representative	
6a. Check only if applicable and check only one box: <input type="checkbox"/> Public-Finance Transaction <input type="checkbox"/> Manufactured-Home Transaction <input type="checkbox"/> A Debtor is a Transmitting Utility	
6b. Check only if applicable and check only one box: <input type="checkbox"/> Agricultural Lien <input type="checkbox"/> Non-UCC Filing	
7. ALTERNATIVE DESIGNATION (if applicable): <input type="checkbox"/> Lessee/Lessor <input type="checkbox"/> Consignee/Consignor <input type="checkbox"/> Seller/Buyer <input type="checkbox"/> Bailee/Belior <input type="checkbox"/> Licensee/Licensor	
8. OPTIONAL FILER REFERENCE DATA:	

CTY# YEAR UCC #  
0602019-09450

**ATTACHMENT A TO UCC FINANCING STATEMENT**  
**DEBTOR: CommWorks Solutions, LLC**  
**SECURED PARTY: Intellectual Ventures Assets 135 LLC**

**"Assigned Patent Rights"** means (a) the patents and patent applications listed below; (b) any future reissues, reexaminations, extensions, continuations, continuing prosecution applications, requests for continuing examinations, divisions, and registrations of any of the items described in (a); (c) rights to apply in any or all countries of the world for future patents, certificates of invention, utility models, industrial design protections, design patent protections, or other future governmental grants or issuances of any type related to any of the items in (a) and/or (b); (d) rights to make, have made, use, sell, offer for sale, import, and otherwise commercialize any product or service under, or on account of, any of the items described in any of the foregoing categories (a), (b), or (c); and (e) exclusive right to bring causes of action and enforcement rights of any kind under, or on account of, any of the items described in any of the foregoing categories (a), (b), or (c), including, without limitation, all causes of action, enforcement rights and all other rights to seek and obtain any other remedies of any kind for past, current and future infringement.

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6832249 (09/860801)	US	12/14/2004 (5/18/2001)	Globally accessible computer network-based broadband communication system with user-controllable quality of information delivery and flow priority  Cisco, Larry
8423630 (10/978953)	US	4/16/2013 (11/1/2004)	Responding to Quality of Service Events in a Multi-Layered Communication System  Steven Reynolds
8812665 (13/781130)	US	8/19/2014 (2/28/2013)	MONITORING FOR AND RESPONDING TO QUALITY OF SERVICE EVENTS IN A MULTI-LAYERED COMMUNICATION SYSTEM  Cisco, Larry
6621854 (08/003996)	US	9/16/2003 (1/15/1993)	Spread-spectrum electromagnetic signals  Bart F. Rice
6711122 (09/500750)	US	3/23/2004 (2/8/2000)	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION  John B. Langley

**ATTACHMENT A TO UCC FINANCING STATEMENT**  
**DEBTOR: CommWorks Solutions, LLC**  
**SECURED PARTY: Intellectual Ventures Assets 135 LLC**



CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7180850 (10/762197)	US	2/20/2007 (1/20/2004)	FREQUENCY OFFSET DIFFERENTIAL PULSE POSITION MODULATION  John B. Langley
7564863 (11/504144)	US	7/21/2009 (8/14/2006)	Frequency offset differential pulse position modulation  Langley, John B.
7626918 (11/504252)	US	12/1/2009 (8/14/2006)	Frequency offset differential pulse position modulation  Michael Mancusi
7609712 (11/504967)	US	10/27/2009 (8/15/2006)	Frequency offset differential pulse position modulation  Michael Mancusi
7062475 (10/715218)	US	6/13/2006 (11/17/2003)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT  Andrew Szabo
7596533 (11/467888)	US	9/29/2009 (8/28/2006)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT  Seth Elliott
RB42232 (11/376700)	US	3/22/2011 (3/15/2006)	RF chipset architecture  Dominik J. Schmidt
6931003 (09/753743)	US	8/16/2005 (12/27/2000)	PACKET PRIORITIZATION PROTOCOL FOR A LARGE-SCALE, HIGH SPEED COMPUTER NETWORK  Keith R. Anderson
7835350 (11/180764)	US	11/16/2010 (7/13/2005)	PRIORITIZING DATA TRANSMISSIONS USING THE NUMBER OF ASSOCIATED ORIGIN ADDRESSES  Keith R. Anderson

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
RE43163 (11/318396)	US	2/7/2012 (12/22/2005)	HIGH-SPEED NETWORK OF INDEPENDENTLY LINKED NODES  Keith R. Anderson
7079823 (09/980027)	US	7/18/2006 (2/27/2002)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION  MORCHE, Dominique
6490067 (09/860078)	US	12/3/2002 (5/16/2001)	MULTI-CHANNEL OPTICAL TRANSCIVER  Scott H. Bloom
6748064 (09/749994)	US	6/8/2004 (12/28/2000)	SYSTEMS AND METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
6636742 (09/599201)	US	10/21/2003 (6/22/2000)	TRACKING OF MOBILE TERMINAL EQUIPMENT IN A MOBILE COMMUNICATIONS SYSTEM  TORKKI, Markus
6868268 (09/896835)	US	3/15/2005 (6/29/2001)	AUDIO CALLING NAME AND NUMBER DELIVERY  James A. Worsham
RE42539 (11/727638)	US	7/12/2011 (3/27/2007)	NETWORK AND METHOD FOR PROVIDING A CALLING NAME TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang
8117068 (12/464782)	US	2/14/2012 (5/12/2009)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK  Brian Mark Shuster

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7412514 (09/932431)	US	8/12/2008 (8/17/2001)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster
7734807 (12/189417)	US	6/8/2010 (8/11/2008)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster
8671216 (12/795597)	US	3/11/2014 (6/7/2010)	METHOD AND APPARATUS FOR IMPROVING BANDWIDTH EFFICIENCY IN A COMPUTER NETWORK  Gary Stephen Shuster
6771971 (09/764696)	US	8/3/2004 (1/18/2001)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC)  Steven W. Smith
7206806 (09/870536)	US	4/17/2007 (5/30/2001)	Method and system for remote utilizing a mobile device to share data objects  Richard A. Pineau
6866587 (09/669479)	US	3/15/2005 (9/25/2000)	WIDE AREA REAL-TIME SOFTWARE ENVIRONMENT  Greg Lane
6427001 (09/874998)	US	7/30/2002 (6/7/2001)	SYSTEM AND METHOD FOR NOTIFICATION OF 911 TELEPHONE CALLS USING LINK MONITORING SYSTEM  Sunil H. Contractor

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0402019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6505163 (09/634794)	US	1/7/2003 (8/9/2000)	NETWORK AND METHOD FOR PROVIDING AN AUTOMATIC RECALL TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang
6721415 (09/506021)	US	4/13/2004 (2/17/2000)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  Quenton Lanny Gilbert
7023978 (10/818817)	US	4/4/2006 (4/6/2004)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  Quenton Lanny Gilbert
6795530 (09/606062)	US	9/21/2004 (6/29/2000)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Lanny Gilbert
RE42122 (11/971456)	US	2/8/2011 (1/9/2008)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Raymond J. Smets
6792094 (09/863477)	US	9/14/2004 (5/23/2001)	INTELLIGENT CALL CONNECTION SERVICE  Mark Kirkpatrick
6754323 (10/025722)	US	6/22/2004 (12/19/2001)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  E-Lee Chang
7363030 (10/852528)	US	4/2/2008 (5/24/2004)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  Linda Ann Roberts

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6967951 (10/044244)	US	11/22/2005 (1/11/2002)	SYSTEM FOR REORDERING SEQUENCED BASED PACKETS IN A SWITCHING NETWORK Vic Alfano
7856011 (11/237482)	US	12/21/2010 (9/27/2005)	Reordering packets Vic Alfano
8107377 (12/759221)	US	1/31/2012 (4/13/2010)	Reordering packets Vic Alfano
8913618 (13/337717)	US	12/16/2014 (12/27/2011)	Reordering packets Vic Alfano
6785534 (09/832011)	US	8/31/2004 (4/11/2001)	PREPAID/POSTPAID AUTOMATIC CHANGE OF PAYMENT OPTION Dara Ung
6754716 (09/502155)	US	6/22/2004 (2/11/2000)	RESTRICTING COMMUNICATION BETWEEN NETWORK DEVICES ON A COMMON NETWORK Rosen Sharma
DE60037651.6 (DE60037651.6)	DE	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
FR1151567 (FR00903718.5)	FR	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
GB1151567 (GB00903718.5)	GB	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen
6678080 (09/923845)	US	1/13/2004 (8/7/2001)	OPTICAL ADD/DROP MULTIPLEXER Ari Tervonen

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7937081 (12/720862)	US	5/3/2011 (3/10/2010)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8200211 (13/097709)	US	6/12/2012 (4/29/2011)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8351924 (13/484583)	US	1/8/2013 (5/31/2012)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8600372 (13/682230)	US	12/3/2013 (11/20/2012)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
8923846 (14/058473)	US	12/30/2014 (10/21/2013)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
9432842 (14/549714)	US	8/30/2016 (11/21/2014)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
9918222 (15/226422)	US	3/13/2018 (8/2/2016)	RECOVERY TECHNIQUES IN MOBILE NETWORKS Heikki Juhani Einola
6665495 (09/698666)	US	12/16/2003 (10/27/2000)	NON-BLOCKING, SCALABLE OPTICAL ROUTER ARCHITECTURE AND METHOD FOR ROUTING OPTICAL TRAFFIC Miles, Larry L.
7145867 (10/114564)	US	12/5/2006 (4/2/2002)	SYSTEM AND METHOD FOR SLOT DEFLECTION ROUTING Aicklen, Gregory H.

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC



CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7184444 (10/138760)	US	2/27/2007 (5/3/2002)	SYSTEM AND METHOD FOR PACKET CLASSIFICATION Posey, Nolan J. JR.
7526203 (10/659485)	US	4/28/2009 (9/10/2003)	Apparatus and method for optical switching at an optical switch fabric Tamil, Lakshman S.
7443790 (11/368867)	US	10/28/2008 (3/6/2006)	System and method for slot deflection routing at optical router/switch Aicklen, Gregory H.
8116315 (11/471149)	US	2/14/2012 (6/20/2006)	SYSTEM AND METHOD FOR PACKET CLASSIFICATION Posey, Nolan J. JR.
7106697 (10/114925)	US	9/12/2006 (4/3/2002)	METHOD FOR DYNAMICALLY COMPUTING A SWITCHING SCHEDULE Robert E. Best
7218637 (10/114928)	US	5/15/2007 (4/3/2002)	System For Switching Data Using Dynamic Scheduling Robert E. Best
7190900 (10/063301)	US	3/13/2007 (4/9/2002)	System and method for implementing dynamic scheduling of data in a non-blocking all-optical switching network Best, Robert E.
7474853 (11/299889)	US	1/6/2009 (12/12/2005)	NON-BLOCKING ALL- OPTICAL SWITCHING NETWORK DYNAMIC DATA SCHEDULING SYSTEM AND IMPLEMENTATION METHOD Robert Best , Ramaswamy Chandrasekaran

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC



CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7496033 (11/453755)	US	02/24/2009 (6/15/2006)	Method for dynamically computing a switching schedule Robert Best
7869427 (11/796682)	US	01/11/2011 (04/27/2007)	SYSTEM FOR SWITCHING DATA USING DYNAMIC SCHEDULING Robert E. Best
7715712 (12/185198)	US	5/11/2010 (08/04/2008)	SYSTEM AND METHOD FOR IMPLEMENTING DYNAMIC SCHEDULING OF DATA IN A NON-BLOCKING ALL-OPTICAL SWITCHING NETWORK Robert E. Best
7124435 (10/040933)	US	10/17/2006 (10/23/2001)	Information management system and method Philippe Richard
7254709 (10/699632)	US	8/7/2007 (11/1/2003)	Managed information transmission of electronic items in a network environment Philippe Richard
8719326 (11/188095)	US	5/6/2014 (7/22/2005)	Adaptive data transformation engine Philippe Richard
9230039 (14/223936)	US	1/5/2016 (3/24/2014)	Adaptive data transformation engine Philippe Richard
6456242 (09/799411)	US	9/24/2002 (3/5/2001)	CONFORMAL BOX ANTENNA James A. Crawford
6433742 (09/693465)	US	8/13/2002 (10/19/2000)	DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS CRAWFORD JAMES A

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6456245 (09/735977)	US	9/24/2002 (12/13/2000)	CARD-BASED DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS  James A. Crawford
6438367 (09/710614)	US	8/20/2002 (11/9/2000)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS  CRAWFORD JAMES A

***"Certain Other Assets"***

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/US2001/016291)	WO	(5/18/2001)	Globally accessible computer network-based broadband communication system with user- controllable quality of information delivery and flow priority  Cisco, Larry
5210770 (07/766372)	US	5/11/1993 (9/27/1991)	MULTIPLE-SIGNAL SPREAD-SPECTRUM TRANSCIEVER  Bart F. Rice
5267271 (07/907358)	US	11/30/1993 (7/1/1992)	Signal analysis technique for determining a subject of binary sequences most likely to have been transmitted in a multi-node communication network  Bart E. Rice
5452328 (08/100334)	US	9/19/1995 (7/30/1993)	Technique for generating sets of binary spreading-code sequences for a high data-rate spread-spectrum network  Bart F. Rice

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
5815526 (08/456077)	US	9/29/1998 (5/31/1995)	Signal comprising binary spreading-code sequences Bart F. Rice
5991333 (09/113410)	US	11/23/1999 (7/10/1998)	Spread-spectrum transceiver Bart F. Rice
7760792 (09/759425)	US	7/20/2010 (1/12/2001)	Spread spectrum electromagnetic signals Bart F. Rice
7457345 (10/873784)	US	11/25/2008 (6/21/2004)	Spread-spectrum transceiver Bart F. Rice
7457348 (11/468923)	US	11/25/2008 (8/31/2006)	Spread-spectrum transceiver Bart F. Rice
7924906 (11/470967)	US	4/12/2011 (9/7/2006)	SPREAD-SPECTRUM RECEIVER Bart F. Rice
(12/755012)	US	(4/6/2010)	SPREAD SPECTRUM TRANSCEIVER Bart F. Rice
7706247 (11/504249)	US	4/27/2010 (8/14/2006)	Frequency offset differential pulse position modulation Michael Mancusi
(09/584057)	US	(5/30/2000)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT Seth Elliott
(11/423847)	US	(6/13/2006)	PERSONALIZED MULTI-SERVICE COMPUTER ENVIRONMENT Seth Elliott

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6710424 (09/962717)	US	3/23/2004 (9/21/2001)	RF CHIPSET ARCHITECTURE Dominik J. Schmidt
6667967 (09/500887)	US	12/23/2003 (2/9/2000)	HIGH-SPEED NETWORK OF INDEPENDENTLY LINKED NODES Richard H. Christensen
(11/147853)	US	(6/8/2005)	SYSTEM AND METHOD FOR DISTRIBUTING ADDRESSES Keith R. Anderson
(11/514294)	US	(8/31/2006)	NEIGHBORHOOD AREA NETWORK WITH RING BACKBONE TOPOLOGY Keith R. Anderson
FR2794311 (FR9906710)	FR	12/14/2007 (5/27/1999)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION MORCHE, Dominique
GB1183777 (GB00936952.1)	GB	7/30/2003 (5/26/2000)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION MORCHE, Dominique
IT1183777 (IT00936952.1)	IT	7/30/2003 (5/26/2000)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION MORCHE, Dominique
7555273 (11/330275)	US	6/30/2009 (1/11/2006)	BAND-PASS FILTER WITH CARRIER FREQUENCY REDUCTION MORCHE, Dominique
(PCT/US2001/015840)	WO	(5/16/2001)	DOUBLE POWER-EYE SAFE LASER OUTPUT ALWAN JAMES J

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(10/287109)	US	(11/1/2002)	MULTI-CHANNEL OPTICAL TRANSCIBIVER  Scott H. Bloom
(PCT/US2001/030144)	WO	(9/27/2001)	SYSTEMS & METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
(11/447279)	US	(6/6/2006)	SYSTEMS AND METHODS FOR LEAST COST ROUTING OF LONG DISTANCE OR INTERNATIONAL TELEPHONE CALLS  Oussama Zbib
(11/256618)	US	(10/21/2005)	TRACKING OF MOBILE TERMINAL EQUIPMENT IN A MOBILE COMMUNICATIONS SYSTEM  TORKKI, Markus
(PCT/US2002/012963)	WO	(4/26/2002)	AUDIO CALLING NAME SERVICE  WORSHAM JAMES A
(11/724311)	US	(3/15/2007)	AUDIO CALLING NAME AND NUMBER DELIVERY  WORSHAM JAMES A
6873686 (09/634793)	US	3/29/2005 (8/9/2000)	NETWORK AND METHOD FOR PROVIDING A CALLING NAME TELECOMMUNICATIONS SERVICE WITH AUTOMATIC SPEECH RECOGNITION CAPABILITY  Zeeman Zhang
(60/213827)	US	(6/23/2000)	Method of cross-promoting and monetizing web sites by means of audio advertisement  Brian Mark Shuster

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(60/213396)	US	(6/23/2000)	Method of delivering audio commercial advertisements Brian Mark Schuster
(60/226108)	US	(8/17/2000)	Method and system of increasing user response to audio advertisements on the internet Brian Mark Shuster
(60/225943)	US	(8/17/2000)	Method and system of enhancing the effectiveness of audio advertisements on the internet Brian Mark Shuster
(09/893362)	US	(6/25/2001)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK Brian Mark Shuster
(13/353787)	US	(1/19/2012)	METHOD AND APPARATUS FOR PROVIDING AUDIO ADVERTISEMENTS IN A COMPUTER NETWORK Brian Mark Shuster
(60/225888)	US	(8/17/2000)	Application and method for maximizing the value of bandwidth usage on wide area networks Gary Stephen Shuster
(60/190646)	US	(3/20/2000)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC) Steven W. Smith
(09/686598)	US	(10/10/2000)	SUBSCRIBER INFORMATION SERVICE CENTER (SISC) Steven W. Smith

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorld Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC



CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/US2002/015636)	WO	(5/17/2002)	Method and system for remote utilizing a mobile device to share data objects  Richard A Pineau
(EP02774105.7)	EP	(5/17/2002)	Method and system for remote utilizing a mobile device to share data objects  Richard A Pineau
(JP2003-500782)	JP	(5/17/2002)	METHOD AND SYSTEM FOR REMOTE UTILIZING A MOBILE DEVICE TO SHARE DATA OBJECTS  Richard A Pineau
(11/725192)	US	(3/15/2007)	WIDE AREA REAL-TIME SOFTWARE ENVIRONMENT  Greg Lane
(PCT/US2001/004776)	WO	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY
(CA2400388)	CA	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY
(EP01909237.8)	EP	(2/15/2001)	TELEPHONE VOICE MESSAGING SYSTEM AND METHOD USING OFF-HOOK IMMEDIATE TRIGGER  GILBERT QUENTON LANNY
6985561 (10/853642)	US	1/10/2006 (5/26/2004)	SYSTEM AND METHOD FOR CUSTOMIZED TELEPHONE GREETING ANNOUNCEMENTS  Raymond J. Smets

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC



CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/US2002/040139)	WO	(12/13/2002)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  CHANG E-LEE
(12/046610)	US	(3/12/2008)	ESTABLISHING A CONFERENCE CALL FROM A CALL-LOG  Linda Ann Roberts
(60/196095)	US	(4/11/2000)	Prepaid/postpaid automatic change of payment option  Dara Ung
FI4119 (FI990238)	FI	8/31/1999 (2/8/1999)	Optical add/drop multiplexer  Ari Tervonen
(PCT/FI2000/000082)	WO	(2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER  Ari Tervonen
EP1151567 (EP00903718.5)	EP	1/2/2008 (2/4/2000)	OPTICAL ADD/DROP MULTIPLEXER  Ari Tervonen
7769374 (09/802861)	US	8/3/2010 (3/12/2001)	RECOVERY TECHNIQUES IN MOBILE NETWORKS  Heikki Juhani Binola
(15/887481)	US	(2/2/2018)	RECOVERY TECHNIQUES IN MOBILE NETWORKS  Heikki Juhani Binola
(10/063268)	US	(4/4/2002)	System and method for implementing dynamic scheduling of data in a non-blocking all-optical switching network  Robert E. Best

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
0602019-09450

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(60/246821)	US	(11/7/2000)	Method and system for passing business objects Marc Asheghian
(10/012240)	US	(11/5/2001)	Method and system for passing business objects Philippe Richard
(60/403873)	US	(8/16/2002)	MANAGED INFORMATION TRANSMISSION IN A NETWORK ENVIRONMENT Phillippe Richard
(60/484885)	US	(7/3/2003)	MANAGED INFORMATION TRANSMISSION OF ELECTRONIC MAIL IN A NETWORK ENVIRONMENT Phillippe Richard
(10/643734)	US	(8/18/2003)	Managed information transmission of electronic items in a network environment Phillippe Richard
(60/590489)	US	(7/22/2004)	Adaptive data transformation engine Phillippe Richard
(PCT/US2001/032613)	WO	(10/18/2001)	DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS CRAWFORD JAMES A
(PCT/US2001/044619)	WO	(11/27/2001)	CARD-BASED DIVERSITY ANTENNA STRUCTURE FOR WIRELESS COMMUNICATIONS James A. Crawford
(PCT/US2001/047183)	WO	(10/30/2001)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS CRAWFORD JAMES A

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 135 LLC

CTY# YEAR UCC #  
 0602019-09450  
**CATHELENE ROBINSON**  
 Clerk of Superior Court  
 Fulton County, Georgia

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
TWI171699  (TW090127391)	TW	1/11/2003  (11/5/2001)	Transmission security for wireless communications  CRAWFORD JAMES A
6650616  (10/178207)	US	11/18/2003  (6/24/2002)	TRANSMISSION SECURITY FOR WIRELESS COMMUNICATIONS  James A. Crawford

ATTACHMENT A TO UCC FINANCING STATEMENT  
 DEBTOR: CommWorks Solutions, LLC  
 SECURED PARTY: Intellectual Ventures Assets 135 LLC

# Exhibit AA

---

**UCC FINANCING STATEMENT**

FOLLOW INSTRUCTIONS

<b>A. NAME &amp; PHONE OF CONTACT AT FILER (optional)</b> <b>UNISEARCH, INC. 360-956-9500</b>
<b>B. E-MAIL CONTACT AT FILER (optional)</b> <b>Kristy.Bertsch@unisearch.com</b>
<b>C. SEND ACKNOWLEDGMENT TO: (Name and Address)</b>  UNISEARCH 1780 BARNES BLVD SW TUMWATER, WA 98512

CTY# YEAR UCC #  
0602019-09451  
Filed and Recorded Dec-05-2019 03:39pm  
CATHELENE ROBINSON  
Clerk of Superior Court  
Fulton County, Georgia

THE ABOVE SPACE IS FOR FILING OFFICE USE ONLY

1. DEBTOR'S NAME: Provide only one Debtor name (1a or 1b) (use exact, full name; do not omit, modify, or abbreviate any part of the Debtor's name); if any part of the individual Debtor's name will not fit in line 1b, leave all of item 1 blank, check here ☐ and provide the individual Debtor information in item 10 of the Financing Statement Addendum (Form UCC1Ad)

1a. ORGANIZATION'S NAME <b>CommWorks Solutions, LLC</b>				
OR	1b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
1c. MAILING ADDRESS	CITY	STATE	POSTAL CODE	COUNTRY
<b>44 Milton Avenue, Suite 254</b>	<b>Alpharetta</b>	<b>GA</b>	<b>30009</b>	<b>USA</b>

2. DEBTOR'S NAME: Provide only one Debtor name (2a or 2b) (use exact, full name; do not omit, modify, or abbreviate any part of the Debtor's name); if any part of the individual Debtor's name will not fit in line 2b, leave all of item 2 blank, check here ☐ and provide the individual Debtor information in item 10 of the Financing Statement Addendum (Form UCC1Ad)

2a. ORGANIZATION'S NAME				
OR	2b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
2c. MAILING ADDRESS	CITY	STATE	POSTAL CODE	COUNTRY

3. SECURED PARTY'S NAME (or NAME of ASSIGNEE of ASSIGNOR SECURED PARTY): Provide only one Secured Party name (3a or 3b)

3a. ORGANIZATION'S NAME <b>Intellectual Ventures Assets 130 LLC</b>				
OR	3b. INDIVIDUAL'S SURNAME	FIRST PERSONAL NAME	ADDITIONAL NAME(S)/INITIAL(S)	SUFFIX
3c. MAILING ADDRESS	CITY	STATE	POSTAL CODE	COUNTRY
<b>251 Little Falls Drive</b>	<b>Wilmington</b>	<b>DE</b>	<b>19808</b>	<b>USA</b>

4. COLLATERAL: This financing statement covers the following collateral:

A first priority security interest in all Collateral to secure all present and future payment and performance obligations of Debtor to Secured Party or any of Secured Party's affiliates, including, without limitation, Debtor's obligations under the PSA (collectively, the "Obligations"). "Collateral" means the Assigned Patent Rights and the Certain Other Assets, and all Revenue (as such term is defined in the PSA).

It is understood and agreed that any Revenue that is properly distributed to either Secured Party or any of Secured Party's Affiliates or Debtor and/or its Affiliates in accordance with the terms and conditions of the PSA are not considered Collateral under this Security Interest Addendum.

Additional Collateral included on Attachment A.

5. Check <u>only</u> if applicable and check <u>only</u> one box: Collateral is <input type="checkbox"/> held in a Trust (see UCC1Ad, item 17 and Instructions) <input type="checkbox"/> being administered by a Decedent's Personal Representative	
6a. Check <u>only</u> if applicable and check <u>only</u> one box: <input type="checkbox"/> Public-Finance Transaction <input type="checkbox"/> Manufactured-Home Transaction <input type="checkbox"/> A Debtor is a Transmitting Utility	6b. Check <u>only</u> if applicable and check <u>only</u> one box: <input type="checkbox"/> Agricultural Lien <input type="checkbox"/> Non-UCC Filing
7. ALTERNATIVE DESIGNATION (if applicable): <input type="checkbox"/> Lessee/Lessor <input type="checkbox"/> Consignee/Consignor <input type="checkbox"/> Seller/Buyer <input type="checkbox"/> Bailee/Bailor <input type="checkbox"/> Licensee/Licensor	
8. OPTIONAL FILER REFERENCE DATA:	

CTY# YEAR UCC #  
0602019-09451

# ATTACHMENT A TO UCC FINANCING STATEMENT

**DEBTOR: CommWorks Solutions, LLC**

**SECURED PARTY: Intellectual Ventures Assets 130 LLC**

"Assigned Patent Rights" means (a) the patents and patent applications listed below; (b) any future reissues, reexaminations, extensions, continuations, continuing prosecution applications, requests for continuing examinations, divisions, and registrations of any of the items described in (a); (c) rights to apply in any or all countries of the world for future patents, certificates of invention, utility models, industrial design protections, design patent protections, or other future governmental grants or issuances of any type related to any of the items in (a) and/or (b); (d) rights to make, have made, use, sell, offer for sale, import, and otherwise commercialize any product or service under, or on account of, any of the items described in any of the foregoing categories (a), (b), or (c); and (e) exclusive right to bring causes of action and enforcement rights of any kind under, or on account of, any of the items described in any of the foregoing categories (a), (b), or (c), including, without limitation, all causes of action, enforcement rights and all other rights to seek and obtain any other remedies of any kind for past, current and future infringement.

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6721787 (09/501204)	US	4/13/2004 (2/10/2000)	SYSTEM AND METHOD FOR WIRELESS HOT-SYNCHRONIZATION OF A PERSONAL DIGITAL ASSISTANT  James Scott Hiscock
JP4294829 (JP2000-125968)	JP	4/17/2009 (4/26/2000)	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION REVISION METHOD  KAKEMIZU MITSUAKI
DE60121094.8 (DE60121094.8)	DE	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
FR1150530 (FR01102111.0)	FR	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
GB1150530 (GB01102111.0)	GB	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6917605 (09/770019)	US	7/12/2005 (1/25/2001)	MOBILE NETWORK SYSTEM AND SERVICE CONTROL INFORMATION CHANGING METHOD  Kakemizu, Mitsuki
8160863 (10/044217)	US	4/17/2012 (11/19/2001)	System and method for connecting a logic circuit simulation to a network  Robert M. Zeidman
7835897 (11/557064)	US	11/16/2010 (11/6/2006)	APPARATUS AND METHOD FOR CONNECTING HARDWARE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
RE42227 (12/481943)	US	3/15/2011 (6/10/2009)	Apparatus and method for connecting hardware to a circuit simulation  Robert Marc Zeidman
8195442 (12/946721)	US	6/5/2012 (11/15/2010)	APPARATUS AND METHOD FOR CONNECTING HARDWARE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
8380481 (13/487750)	US	2/19/2013 (6/4/2012)	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
7069483 (10/437128)	US	6/27/2006 (5/13/2003)	System and method for identifying nodes in a wireless mesh network  Michael P. Nova
JP4874550 (JP2004-572210)	JP	12/2/2011 (10/31/2003)	System and method for routing packets in a wired or wireless network  GILLIES DONALD W



CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
JP4369374 (JP2004-572211)	JP	11/18/2009 (10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  WANG WEILIN
7852796 (11/420668)	US	12/14/2010 (5/26/2006)	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION  Xudong Wang
7835372 (11/421998)	US	11/16/2010 (6/2/2006)	System and Method for Transparent Wireless Bridging of Communication Channel Segments  Weilin Wang
7451365 (11/425114)	US	11/11/2008 (6/19/2006)	System and Method for Identifying Nodes in a Wireless Network  Donald W. Gillies
7957356 (11/462663)	US	6/7/2011 (8/4/2006)	SCALABE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Xudong Wang
7941149 (11/615582)	US	5/10/2011 (12/22/2006)	Multi-Hop Ultra Wide Band Wireless Network Communication  Weilin Wang
8175613 (11/741630)	US	5/8/2012 (4/27/2007)	SYSTEMS AND METHODS FOR DETERMINING LOCATION OF DEVICES WITHIN A WIRELESS NETWORK  Chao Gui
8780770 (11/741637)	US	7/15/2014 (4/27/2007)	SYSTEMS AND METHODS FOR VOICE COMMUNICATION OVER A WIRELESS NETWORK  Weiguang Shi

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
8611320 (12/950558)	US	12/17/2013 (11/19/2010)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS Weilin Wang
9554304 (14/090760)	US	1/24/2017 (11/26/2013)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS Xudong Wang
9930575 (15/409896)	US	3/27/2018 (1/19/2017)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS Weilin Wang
7092986 (10/067278)	US	8/15/2006 (2/7/2002)	Transparent mobile IPv6 agent Wang, Mei Na
RB43704 (12/608732)	US	10/2/2012 (10/29/2009)	Determining and provisioning paths within a network of communication elements Gupta, Sanyogita
7760664 (11/101136)	US	7/20/2010 (4/7/2005)	Determining and provisioning paths in a network Sanyogita Gupta
CA2581734 (CA2581734)	CA	8/28/2012 (9/28/2005)	Determining and provisioning paths in a network Sanyogita Gupta
DE602005053126.2 (DE602005053126.2)	DE	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network Sanyogita Gupta
GB1797670 (GB05857725.5)	GB	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network Sanyogita Gupta
JP4777990 (JP2007-534687)	JP	7/8/2011 (9/28/2005)	Determining and provisioning paths in a network Sanyogita Gupta

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 130 LLC  
Page 4 of 23

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6836466 (09/579371)	US	12/28/2004 (5/26/2000)	Method and system for measuring IP performance metrics Krishna Kant
6775253 (09/512644)	US	8/10/2004 (2/24/2000)	Adaptive signaling for wireless packet telephony Prathima Agrawal
6628943 (09/512645)	US	9/30/2003 (2/24/2000)	Mobility management utilizing active address propagation Prathima Agrawal
6788660 (09/512646)	US	9/7/2004 (2/24/2000)	Adaptive mobile signaling for wireless internet telephony Prathima Agrawal
6487406 (09/545619)	US	11/26/2002 (4/10/2000)	PCS-to-mobile IP internetworking Li-Fung Chang
TWI183532 (TW089110383)	TW	8/11/2003 (5/29/2000)	PCS-to-mobile IP internetworking Chang, Li-Fung
CA2310783 (CA2310783)	CA	2/3/2004 (6/6/2000)	PCS-to-mobile IP internetworking Chang, Li-Fung
6490259 (09/512514)	US	12/3/2002 (2/24/2000)	Active link layer and intra-domain mobility for IP networks AGRAWAL PRATHIMA
RE42883 (12/001975)	US	11/1/2011 (12/13/2007)	Enhanced Phone-Based Collaboration Korycki, Jacek
6985724 (10/239763)	US	1/10/2006 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 130 LLC  
Page 5 of 23

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6857007 (09/723349)	US	2/15/2005 (11/27/2000)	Personal digital assistant facilitated communication system Bloomfield, Mark C.
8224909 (12/369785)	US	7/17/2012 (2/12/2009)	Personal digital assistant facilitated communication system Bloomfield, Mark C.
8533278 (13/490403)	US	9/10/2013 (6/6/2012)	Mobile computing device based communication systems and methods Mark C. Bloomfield
6891807 (10/341847)	US	5/10/2005 (1/13/2003)	Time based wireless access provisioning Roskind, James A.
7177285 (10/961959)	US	2/13/2007 (10/8/2004)	Time based wireless access provisioning Roskind, James A.
7463596 (11/673513)	US	12/9/2008 (2/9/2007)	TIME BASED WIRELESS ACCESS PROVISIONING Roskind, James A.
7911979 (12/323399)	US	3/22/2011 (11/25/2008)	Time Based Access Provisioning System and Process James A. Roskind
7051116 (09/983042)	US	5/23/2006 (10/22/2001)	Client device identification when communicating through a network address translator device Rodriguez-Val, Richard
7484005 (11/351116)	US	1/27/2009 (2/10/2006)	Client device identification when communicating through a network address translator device Richard Rodriguez-Val

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7814230 (12/337854)	US	10/12/2010 (12/18/2008)	Client device identification when communicating through a network address translator device  Rodriguez-Val, Richard
6775258 (09/527786)	US	8/10/2004 (3/17/2000)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system  Van Valkenburg, Sander
6865237 (09/676373)	US	3/8/2005 (9/29/2000)	Method and system for digital signal transmission  Boariu, Adrian
7006579 (10/023924)	US	2/28/2006 (12/18/2001)	ISI-robust slot formats for non-orthogonal-based space-time block codes  Kuchi, Kiran
DE60123282.8 (DE01273305.1)	DE	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
GB1350354 (GB01273305.1)	GB	9/20/2006 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
8031800 (10/450997)	US	10/4/2011 (12/19/2001)	Transmitting digital signal  Tirkkonen, Olav
DE60244331.8 (DE60244331.8)	DE	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav
FR1405453 (FR02743313.5)	FR	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav
GB1405453 (GB02743313.5)	GB	1/2/2013 (6/24/2002)	Transmission method  Tirkkonen, Olav

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
7460609 (10/739017)	US	12/2/2008 (12/19/2003)	Transmission method using complex channel symbols Tirkkonen, Olav
7355961 (11/070624)	US	4/8/2008 (3/2/2005)	Method and arrangement for digital signal transmission using layered space-time codes Tirkkonen, Olav
RE43746 (13/166702)	US	10/16/2012 (6/22/2011)	Method and radio system for digital signal transmission using complex space-time codes Tirkkonen, Olav
7061379 (10/301846)	US	6/13/2006 (11/21/2002)	RFID system and method for ensuring safety of hazardous or dangerous substances Chen, Fung-Jou
6724883 (09/660133)	US	4/20/2004 (9/12/2000)	Processing of data message in a network element of a communications network Lehtinen, Pekka
CNZL00808958.2 (CN00808958.2)	CN	11/10/2004 (6/13/2000)	INITIATING A CONTROLLING SERVICE Tuunanen, Heikki
DE60042650.5 (DE60042650.5)	DE	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE Tuunanen, Heikki
ES1192811 (ES00942154.6)	ES	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE Tuunanen, Heikki

CTY# YEAR UCC#  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
GB1192811 (GB00942154.6)	GB	7/29/2009 (6/13/2000)	Call set-up control in an intelligent network by conditional initiation of more than one controlling service Tuunanen, Heikki
IT1192811 (IT00942154.6)	IT	7/29/2009 (6/13/2000)	INITIATING A CONTROLLING SERVICE Tuunanen, Heikki
6594356 (10/014918)	US	7/15/2003 (12/14/2001)	Initiating a controlling service Tuunanen, Heikki
7027465 (10/167986)	US	4/11/2006 (6/11/2002)	Method for contention free traffic detection Hautala Petri
RE44904 (13/171882)	US	5/20/2014 (6/29/2011)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION Hautala Petri
7209950 (09/921167)	US	4/24/2007 (8/2/2001)	Method and apparatus for a network independent short message delivery system Simon Bennett
7224642 (11/340733)	US	5/29/2007 (1/26/2006)	Wireless sensor data processing systems Bao Q. Tran
6980089 (09/924730)	US	12/27/2005 (8/8/2001)	Non-intrusive coupling to shielded power cable Paul A. Kline
7245201 (10/947929)	US	7/17/2007 (9/23/2004)	Power line coupling device and method of using the same Paul A. Kline
7248148 (11/265230)	US	7/24/2007 (11/3/2005)	Power line coupling device and method of using the same Paul A. Kline



CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
6956941 (09/547627)	US	10/18/2005 (4/12/2000)	METHOD AND SYSTEM FOR SCHEDULING INBOUND INQUIRIES Daniel N. Duncan
6859529 (10/082386)	US	2/22/2005 (2/25/2002)	Method and system for self-service scheduling of inbound inquiries Daniel N. Duncan
6456764 (09/668372)	US	9/24/2002 (9/25/2000)	Optical directional coupler Hideaki Okayama
6804713 (09/549687)	US	10/12/2004 (4/14/2000)	Operational supervisory system for a server Miwa Nishio
6335821 (09/501606)	US	1/1/2002 (2/10/2000)	Optical fiber amplifier and a method for controlling the same Mikiya Suzuki
6483634 (09/662904)	US	11/19/2002 (9/15/2000)	Optical amplifier Andrew R Pratt
6427037 (09/497235)	US	7/30/2002 (2/3/2000)	Two-stage optical switch circuit network Hideaki Okayama
6901437 (09/684047)	US	5/31/2005 (10/6/2000)	Mobile cache for dynamically composing user- specific information Benjamin Bin Li
9648122 (11/133755)	US	5/9/2017 (5/19/2005)	Mobile cache for dynamically composing user- specific information Benjamin Bin Li
10051077 (15/486546)	US	8/14/2018 (4/13/2017)	Mobile cache for dynamically composing user- specific information Benjamin Bin Li

CTY# YEAR UCC #  
0602019-09451

**"Certain Other Assets"**

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
BP1150530 (BP01102111.0)	BP	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
SE1150530 (SE01102111.0)	SE	6/28/2006 (1/31/2001)	Mobile network system and service control information changing method  KAKEMIZU MITSUAKI (JP)
(60/193169)	US	(3/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7050962 (09/751573)	US	5/23/2006 (12/28/2000)	Method for connecting a hardware emulator to a network  Robert M. Zeidman
7266490 (10/158648)	US	9/4/2007 (5/31/2002)	Apparatus and method for connecting hardware to a circuit simulation  Robert Marc Zeidman
(10/158772)	US	(5/31/2002)	Apparatus and method for connecting a hardware emulator to a computer peripheral  Robert Marc Zeidman
(11/557057)	US	(11/6/2006)	APPARATUS AND METHOD FOR CONNECTING A HARDWARE EMULATOR TO A COMPUTER PERIPHERAL  Robert Marc Zeidman
(11/557053)	US	(11/6/2006)	SYSTEM AND METHOD FOR CONNECTING A LOGIC CIRCUIT SIMULATION TO A NETWORK  Robert M. Ziedman

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(13/766960)	US	(2/14/2013)	CONVEYING DATA FROM A HARDWARE DEVICE TO A CIRCUIT SIMULATION  Robert Marc Zeidman
(60/380425)	US	(5/13/2002)	Low cost, minimal software footprint, self configuring, ad hoc, autonomic networking apparatus and method of use  Michael P. Nova
(10/437129)	US	(5/13/2003)	SYSTEMS AND METHODS FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  Michael P. Nova
(PCT/US2003/034799)	WO	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W
(CN200380110363.0)	CN	(10/31/2003)	System and method for routing packets in a wired or wireless network  GILLIES DONALD W WANG WEILIN N
(BP03778062.4)	EP	(10/31/2003)	SYSTEM AND METHOD FOR ROUTING PACKETS IN A WIRED OR WIRELESS NETWORK  GILLIES DONALD W
(PCT/US2003/034884)	WO	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF A WIRED OR WIRELESS NETWORK  NOVA MICHAEL P
(CN200380110362.6)	CN	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  GILLIES DONALD W WANG WEILIN N

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 130 LLC  
Page 12 of 23

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(EP03778075.6)	EP	(10/31/2003)	SYSTEM AND METHOD FOR BOUNDARY SCAN TEST OF WIRED OR WIRELESS NETWORK  WANG WEILIN
(60/557954)	US	(3/31/2004)	Broadband applications for wireless mesh networks  Weilin Wang
(10/816481)	US	(4/1/2004)	Systems and methods for congestion control in a wireless mesh network  Michael P. Nova
(11/076738)	US	(3/9/2005)	Distributed TDMA for wireless mesh network  Weilin Wang
(11/095349)	US	(3/31/2005)	SYSTEMS AND METHODS FOR BROADBAND DATA COMMUNICATION IN A WIRELESS MESH NETWORK  Weilin Wang
(60/747409)	US	(5/16/2006)	Distributed Multi-Channel TDMA MAC for Wireless Mesh Networks  Xudong Wang
(PCT/US2007/069031)	WO	(5/16/2007)	DISTRIBUTED MULTICHANNEL WIRELESS COMMUNICATION  GUI CHAO
(PCT/US2007/070225)	WO	(6/1/2007)	SYSTEM AND METHOD FOR TRANSPARENT WIRELESS BRIDGING OF COMMUNICATION CHANNEL SEGMENTS  RIMMER JAMES

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(15/935928)	US	(3/26/2018)	SCALABLE MEDIA ACCESS CONTROL FOR MULTI-HOP HIGH BANDWIDTH COMMUNICATIONS  Weilin Wang
7289456 (10/118187)	US	10/30/2007 (4/8/2002)	Determining and provisioning paths within a network of communication elements  Gupta, Sanyogita
(60/614609)	US	(9/30/2004)	Modeling of topology connectivity map for efficient layer 1 routing  Sanyogita Gupta
(PCT/US2005/034418)	WO	(9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
EP1797670 (EP05857725.5)	EP	11/22/2017 (9/28/2005)	Determining and provisioning paths in a network  Sanyogita Gupta
(60/121552)	US	(2/25/1999)	Adaptive mobility-aware signaling for wireless IP telephony  Agrawal, Prathima
(PCT/US2000/004629)	WO	(2/24/2000)	Adaptive signaling and mobility for wireless telephony  Agrawal, Prathima
(60/139471)	US	(6/16/1999)	PCS-to-mobile IP internetworking  Chang, Li-Fung
(PCT/US2000/014059)	WO	(5/22/2000)	ACTIVE LINK LAYER AND INTRA- DOMAIN MOBILITY FOR IP NETWORKS  AGRAWAL PRATHIMA

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(60/485880)	US	(7/8/2003)	Enhanced Phone-Based Collaboration Korycki, Jacek
6975622 (10/756526)	US	12/13/2005 (1/13/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
(PCT/US2004/021407)	WO	(7/2/2004)	Enhanced Phone-Based Collaboration Korycki, Jacek
SE522377 (SE0001148-6)	SE	2/3/2004 (3/31/2000)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
(PCT/SE2001/000423)	WO	(2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
EP1269688 (EP01910283.9)	EP	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
DE60145827.3 (DE60145827.3)	DE	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno
FR1269688 (FR01910283.9)	FR	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes Fredriksson, Lars-Berno

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
GB1269688 (GB01910283.9)	GB	12/21/2011 (2/27/2001)	Device for transmitting data and control commands via radio connections in a distributed control system for one or more machines and/or processes  Fredriksson, Lars-Berno
(60/229317)	US	(8/30/2000)	Personal digital assistant based communication system  Bloomfield, Mark C.
(PCT/US2001/023402)	WO	(7/26/2001)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(10/681562)	US	(10/8/2003)	Personal digital assistant facilitated communication system  Bloomfield, Mark C.
(PCT/US1997/018071)	WO	(10/7/1997)	Unable to verify  Unable to Verify
(PCT/US2004/000860)	WO	(1/13/2004)	Time based wireless access provisioning  Roskind, James A.
(10/542183)	US	(7/13/2005)	Time based wireless access provisioning  Roskind, James
(60/299454)	US	(6/21/2001)	Client device identification when communicating through a network address translator device  Rodriguez-Val, Richard
(EP01912047.6)	EP	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system  Van Valkenburg, Sander



CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/IB2001/000352)	WO	(3/13/2001)	Apparatus, and associated method, for routing packet data in an ad hoc, wireless communication system  Van Valkenburg, Sander
FI112565 (FI20000406)	FI	2003-12-15_Salesforce (2/22/2000)	METHOD AND RADIO SYSTEM FOR DIGITAL SIGNAL TRANSMISSION  HOTTINEN,ARI
(60/193402)	US	(3/29/2000)	Class of space-time block codes for more than two transmit antennas  Boariu, Adrian
(FI20001944)	FI	(9/4/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
(PCT/FI2000/000916)	WO	(10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
EP1336268 (EP00969617.0)	BP	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
DE60048671.0 (DE60048671.0)	DE	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
FR11336268 (FR00969617.0)	FR	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav
GB1336268 (GB00969617.0)	GB	7/23/2014 (10/23/2000)	Method and arrangement for digital signal transmission  Tirkkonen, Olav

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(FI20002845)	FI	(12/22/2000)	Transmitting digital signal Tirkkonen, Olav
(PCT/FI2001/000166)	WO	(2/20/2001)	Method and radio system for digital signal transmission Tirkkonen, Olav
(EP01911785.2)	EP	(2/20/2001)	Method and radio system for digital signal transmission Tirkkonen, Olav
(FI20011357)	FI	(6/25/2001)	Transmitting digital signal Tirkkonen, Olav
(PCT/FI2001/001133)	WO	(12/19/2001)	Transmitting digital signal Tirkkonen, Olav
EP1350354 (EP01273305.1)	EP	9/20/2006 (12/19/2001)	Transmitting digital signal Tirkkonen, Olav
(PCT/FI2002/000553)	WO	(6/24/2002)	Transmission method Tirkkonen, Olav
EP1405453 (EP02743313.5)	EP	1/2/2013 (6/24/2002)	Transmission method Tirkkonen, Olav
(10/225457)	US	(8/22/2002)	Method and radio system for digital signal transmission Ari Hottinen
(10/378068)	US	(3/4/2003)	Method and arrangement for digital signal transmission Tirkkonen, Olav
7477703 (11/070717)	US	1/13/2009 (3/2/2005)	Method and radio system for digital signal transmission using complex space-time codes Tirkkonen, Olav

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 130 LLC  
Page 18 of 23

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(MX03009987)	MX	(10/31/2003)	RFID system and method for ensuring safety of hazardous or dangerous substances Reade, Walter Caswell
FI106507 (FI980824)	FI	2/15/2001 (4/9/1998)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
(PCT/FI1999/000300)	WO	(4/9/1999)	PROCESSING OF DATA MESSAGE IN A NETWORK ELEMENT OF A COMMUNICATIONS NETWORK LEHTINEN PEKKA
FI108604 (FI990963)	FI	2/15/2002 (4/28/1999)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka
(PCT/FI2000/000359)	WO	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka
(BP00920786.1)	EP	(4/26/2000)	METHOD FOR MANAGING MOBILE STATION FACILITIES Wallenius, Jukka
6975855 (09/958065)	US	12/13/2005 (4/26/2000)	Method for managing mobile station facilities Wallenius, Jukka
FI108979 (FI991360)	FI	4/30/2002 (6/14/1999)	INITIATING A CONTROLLING SERVICE Tuunanen, Heikki
(PCT/FI2000/000530)	WO	(6/13/2000)	INITIATING A CONTROLLING SERVICE Tuunanen, Heikki

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
EP1192811 (EP00942154.6)	EP	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
FR1192811 (FR00942154.6)	FR	7/29/2009 (6/13/2000)	CALL SET-UP CONTROL IN AN INTELLIGENT NETWORK BY CONDITIONAL INITIATION OF MORE THAN ONE CONTROLLING SERVICE  Tuunanen, Heikki
(JP2001-504184)	JP	(6/13/2000)	INITIATING A CONTROLLING SERVICE  Tuunanen, Heikki
FI109506 (FI981113)	FI	8/15/2002 (5/9/1998)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
(PCT/FI1999/000430)	WO	(5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
CN9806247.2 (CN99806247.2)	CN	2/18/2004 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
EP1080587 (EP99952144.6)	EP	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  HUOTARI SEPPO

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
DE69934114.0 (DE69934114.0)	DE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
ES1080587 (ES99952144.6)	ES	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
FR1080587 (FR99952144.6)	FR	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
GB1080587 (GB99952144.6)	GB	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
IT1080587 (IT99952144.6)	IT	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
NL1080587 (NL99952144.6)	NL	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
SE1080587 (SE99952144.6)	SE	11/22/2006 (5/18/1999)	A METHOD OF MANAGING A SUBSCRIBER SERVICE BY MEANS OF AN INTELLIGENT NETWORK SERVICE  Huotari, Seppo
6341221 (09/702495)	US	1/22/2002 (10/31/2000)	Method of managing a subscriber service by an intelligent network service  Huotari, Seppo

ATTACHMENT A TO UCC FINANCING STATEMENT  
DEBTOR: CommWorks Solutions, LLC  
SECURED PARTY: Intellectual Ventures Assets 130 LLC  
Page 21 of 23

CTY# YEAR UCC #  
0602019-09451

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/EP1999/010097)	WO	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION Hautala Petri
(EP99965493.2)	EP	(12/17/1999)	A METHOD FOR CONTENTION FREE TRAFFIC DETECTION Hautala Petri
7555014 (11/402621)	US	6/30/2009 (4/11/2006)	METHOD FOR CONTENTION FREE TRAFFIC DETECTION Hautala Petri
(60/225603)	US	(8/15/2000)	Cellular network independent short message delivery system Simon Bennett
(PCT/US2001/024475)	WO	(8/2/2001)	Method And Apparatus For A Network Independent Short Message Delivery System Simon Bennett
(11/741894)	US	(4/30/2007)	Wireless sensor data processing systems Bao Q. Tran
(60/224031)	US	(8/9/2000)	Non-intrusive coupler for a broadband communications system using high voltage shielded power distributed cables Paul A. Kline
(PCT/US2005/041148)	WO	(11/14/2005)	Power line coupling device and method of using the same William O. Radtke
(EP05849637.3)	EP	(11/14/2005)	Power line coupling device and method of using the same William O. Radtke

CTY# YEAR UCC #  
0602019-09451  
**CATHELENE ROBINSON**  
Clerk of Superior Court  
Fulton County, Georgia

Patent/ Application Number	Country	Issue Date/ Filing Date	Title of Patent and Inventor(s)
(PCT/US2001/011311)	WO	(4/6/2001)	Method and system for scheduling inbound inquiries  Daniel N. Duncan
JP3810956  (JP11-212974)	JP	6/2/2006  (7/28/1999)	Operational supervisory system for a server  Miwa Nishio